世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 **H04L 9/08, 9/32, 12/28, H04H 1/00, H04N 7/167**	**A1**	(11) 国際公開番号	**WO00/62475**
		(43) 国際公開日	2000年10月19日(19.10.00)

(21) 国際出願番号 PCT/JP00/02353

(22) 国際出願日 2000年4月11日(11.04.00)

(30) 優先権データ

特願平11/105966 1999年4月13日(13.04.99) JP

特願平11/143988 1999年5月24日(24.05.99) JP

(71) 出願人（米国を除くすべての指定国について）
ソニー株式会社(SONY CORPORATION)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
浅野智之(ASANO, Tomoyuki)[JP/JP]
大澤義知(OSAWA, Yoshitomo)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号
ソニー株式会社内 Tokyo, (JP)
(74) 代理人
小池 晃, 外(KOIKE, Akira et al.)
〒105-0001 東京都港区虎ノ門二丁目6番4号
第11森ビル Tokyo, (JP)

(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

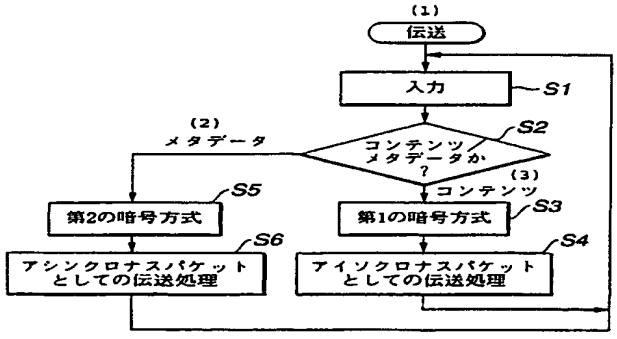
添付公開書類
国際調査報告書

(54)Title: **INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING DEVICE**

(54)発明の名称 情報処理システム、情報処理方法及び情報処理装置

(57) Abstract

Protocol for mutual authentication and for sharing a plurality of encryption keys is practiced between a CPU (12) on a data transmitter (10) side and a CPU (22) on a data receiver (20) side prior to data transmission. The data transmitter (10) encrypts data which requires assurance of a transmission band with a first encryption key by the CPU (12) and transmits it through an input/output interface (16) in a first transmission mode. The data transmitter (10) further encrypts related data concerning the above mentioned data with a second encryption key through the input/output interface (16) in a second transmission mode. The data receiver (20) decrypts the data which requires the assurance of the transmission band and is received through an input/output interface (24) in the first transmission mode with the first code key and decrypts the related data which are received through the input/output interface (24) in the second transmission mode with the second code key.



S1...INPUT
S2...CONTENTS OR META-DATA?
S3...1ST ENCRYPTION METHOD
S4...TRANSMIT DATA AS ISOCHRONOUS PACKET
S5...2ND ENCRYPTION METHOD
S6...TRANSMIT DATA AS ASYNCHRONOUS PACKET
(1)...TRANSMISSION
(2)...META-DATA
(3)...CONTENTS

(57)要約

データ送信装置１０側のＣＰＵ１２とデータ受信装置２０側のＣＰＵ２２との間で、データ伝送に先立って、相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する。データ送信装置１０は、伝送帯域の保証が必要なデータを上記ＣＰＵ１２により第１の暗号鍵で暗号化して第１の伝送モードで入出力インターフェース１６を介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記入出力インターフェース１６を介して送信し、上記データ受信装置２０は、上記ＣＰＵ２２により、入出力インターフェース２４を介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記入出力インターフェース２４を介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する。

明細書

情報処理システム、情報処理方法及び情報処理装置

技術分野

本発明は、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介してデータの伝送を行う情報処理システム、情報処理方法及び情報処理装置に関する。

背景技術

近年、例えば家庭内において、複数のＡＶ機器をデジタルインターフェースを介して接続し、音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたシステムが普及しつつある。

例えば、デジタルバスであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス（以下、単にＩＥＥＥ１３９４シリアルバスという）のインターフェースを持つビデオカメラやＤＶＤプレーヤなどの機器では、データを高品質で記録することが可能であ

ることから、著作権のあるデータが不正にコピーされてしまうのを防止する必要がある。

例えば、光磁気ディスク装置に映画情報を記録することが許可されているか否かを表す情報を記憶しておき、この情報を利用して、その光磁気ディスク装置が正当な装置すなわち著作権者からのライセンスを受けた装置であるか否かを認証するようにし、正当な装置として認証された光磁気ディスク装置のみに映画情報の記録を許可するようにすることが行われる。このような場合、映画情報を伝送する側の装置（以下、このような装置をソース(source)という）と、伝送を受けた装置（以下、このような装置をシンク(sink)という）との間で、相手側の装置が適正な装置であるか否かを認証する必要がある。

このようなシステムにおける著作権保護を目的として、様々な認証方式が提案されている。これらの認証方式に用いられる認証プロトコルには、暗号アルゴリズムが用いられることが多い。

ところで、音楽データを機器間で伝送する際には、例えば、音楽データの伝送途中に伝送が止まったり、伝送できるデータ量が極端に減ったりすると、受信側で音楽の再生に必要なデータが得られなくなり、音楽が途切れてしまうおそれがあるので、ある程度の帯域を確保した状態で音楽データを伝送する必要がある。

一方、音楽データそのものではないが、音楽データに関連した情報として、例えば歌詞やアーティストの写真などを伝送する場合には、音楽データそのもの伝送する場合に比べて、リアルタイム性を必要としないので、伝送帯域が確保されていない伝送方式を用いて伝送することが可能である。一般に、伝送帯域が確保されていない

伝送方式を用いる方が、伝送路全体の帯域を消費しないという点で望まれることが多い。

発明の開示

そこで、本発明の目的は、上述の如き従来の問題点に鑑み、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の２種類の伝送方式を採用して、データを確実に伝送することができるようにした情報処理システム、情報処理方法、情報処理装置を提供することにある。

また、本発明の他の目的は、伝送帯域の保証が必要なデータと上記データに関する関連データを異なる暗号鍵により暗号化して安全に伝送することができるようにした情報処理システム、情報処理方法、情報処理装置を提供することにある。

さらに、本発明の他の目的は、送信側の情報処理装置と受信側の情報処理装置が互いの正当性を認証するとともに、暗号鍵を共有することができるようにした情報処理システム、情報処理方法、情報処理装置を提供することにある。

本発明に係る情報処理システムは、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記インターフェースを介して送信する

送信制御手段とを備える第１の情報処理装置と、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記インターフェースを介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する受信制御手段とを備える第２の情報処理装置とを具備することを特徴とする。

また、本発明は、第１の情報処理装置と第２の情報処理装置との間で伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介してデータ伝送を行う情報処理方法であって、上記第１の情報処理装置から伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで送信するとともに、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで送信し、上記第２の情報処理装置側で第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号することを特徴とする。

また、本発明に係る情報処理装置は、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記インターフェースを介して送信する送信制御手段とを備えることを特徴とする。

さらに、本発明に係る情報処理装置は、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記インターフェースを介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する受信制御手段とを備えることを特徴とする。

図面の簡単な説明

図１は、本発明を適用したＡＶシステムを含むデジタル衛星放送システムの全体構成をブロック図である。

図２は、上記デジタル衛星放送システムにおける地上局の構成を示すブロック図である。

図３は、上記地上局から送信されるデータを示す図である。

図４Ａ～図４Ｈは、送信データの時分割多重化構造を示す説明図である。

図５は、本発明を適用したデータ伝送システムの構成を示すブロック図である。

図６は、ＩＥＥＥ１３９４バスケーブルの構造を模式的に示す説明図である。

図７Ａ～図７Ｃは、ＩＥＥＥ１３９４における信号伝送形態を示す説明図である。

図８は、ＩＥＥＥ１３９４におけるＰａｃｋｅｔ送信の概要を示

す説明図である。

図９は、上記データ伝送システムにおけるデータ送信装置の要部構成を示すブロック図である。

図１０は、上記データ送信装置の動作を示すフローチャートである。

図１１は、上記データ伝送システムにおけるデータ伝送の手順を示すフローチャートである。

図１２は、上記データ伝送システムにおけるデータ送信装置側の処理手順を示すフローチャートである。

図１３は、上記データ伝送システムにおけるデータ受信装置側の処理手順を示すフローチャートである。

図１４は、上記データ伝送システムにおけるデータ伝送の他の手順を示すフローチャートである。

図１５は、上記データ伝送システムにおけるデータ送信装置側の他の処理手順を示すフローチャートである。

図１６は、上記データ伝送システムにおけるデータ受信装置側の他の処理手順を示すフローチャートである。

発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

本発明は、各種デジタルＡＶ(Audio Visual)機器やパーソナルコンピュータ装置等の電子機器を、例えばＩＥＥＥ(Institute of El

ectrical Engineers）１３９４バスを介して相互に接続することで、機器間でデータを送受信できるようにしたデータ伝送システム（ＡＶシステム）に適用される。このＡＶシステムは、デジタル衛星放送を受信して、受信データをダウンロード可能な構成が採られるものである。

このＡＶシステムを含むデジタル衛星放送システムの全体構成を図１に示してある。

この図１に示したデジタル衛星放送システムにおいて、デジタル衛星放送の地上局１０１には、テレビ番組素材サーバ１０６からのテレビ番組放送のための素材と、楽曲素材サーバ１０７からの楽曲データの素材と、音声付加情報サーバ１０８からの音声付加情報と、ＧＵＩ(Graphical User Interface)データサーバ１０９からのＧＵＩデータとが送られる。

テレビ番組素材サーバ１０６は、通常の放送番組の素材を提供するサーバである。このテレビ番組素材サーバから送られてくる音楽放送の素材は、動画及び音声とされる。例えば、音楽放送番組であれば、上記テレビ番組素材サーバ１０６の動画及び音声の素材を利用して、例えば新曲のプロモーション用の動画及び音声が放送されたりすることになる。

楽曲素材サーバ１０７は、オーディオチャンネルを使用して、オーディオ番組を提供するサーバである。このオーディオ番組の素材は音声のみとなる。この楽曲素材サーバ１０７は、複数のオーディオチャンネルのオーディオ番組の素材を地上局１０１に伝送する。

各オーディオチャンネルの番組放送ではそれぞれ同一の楽曲が所定の単位時間繰り返して放送される。各オーディオチャンネルは、

それぞれ、独立しており、その利用方法としては各種考えられる。例えば、１つのオーディオチャンネルでは最新の日本のポップスの数曲を或る一定時間繰り返し放送し、他のオーディオチャンネルでは最新の外国のポップスの数曲を或る一定時間繰り返し放送するというようにされる。

音声付加情報サーバ１０８は、楽曲素材サーバ１０７から出力される楽曲の演奏時間等を提供するサーバである。

ＧＵＩデータサーバ１０９は、ユーザが操作に用いるＧＵＩ画面を形成するための「ＧＵＩデータ」を提供する。例えば後述するような楽曲のダウンロードに関するＧＵＩ画面であれば、配信される楽曲のリストページや各楽曲の情報ページを形成するための画像データ、テキストデータ、アルバムジャケットの静止画を形成するためのデータなどを提供する。さらには、ＡＶシステム１０３側にていわゆるＥＰＧ(Electrical Program Guide)といわれる番組表表示を行うのに利用されるＥＰＧデータもここから提供される。

なお、「ＧＵＩデータ」としては、例えばＭＨＥＧ(Multimedia Hypermedia Information Coding Experts Group)方式が採用される。ＭＨＥＧとは、マルチメディア情報、手順、操作などのそれぞれと、その組合せをオブジェクトとして捉え、それらのオブジェクトを符号化した上で、タイトル（例えばＧＵＩ画面）として制作するためのシナリオ記述の国際標準である。また、このデジタル衛星放送システムではＭＨＥＧ－５を採用するものとする。

地上局１０１は上記テレビ番組素材サーバ１０６、楽曲素材サーバ１０７、音声付加情報サーバ１０８及びＧＵＩデータサーバ１０９から伝送された情報を多重化して送信する。

このデジタル衛星放送システムでは、テレビ番組素材サーバ１０６から伝送されたビデオデータはＭＰＥＧ(Moving Picture Experts Group)２方式により圧縮符号化され、オーディオデータはＭＰＥＧ２オーディオ方式により圧縮符号化される。また、楽曲素材サーバ１０７から伝送されたオーディオデータは、オーディオチャンネルごとに対応して、例えばＭＰＥＧ２オーディオ方式と、ＡＴＲＡＣ(Adoptive Tranform Acoustic Coding) 方式の何れか一方の方式により圧縮符号化される。

また、これらのデータは多重化の際、キー情報サーバ１１０からのキー情報を利用して暗号化される。

地上局１０１からの信号は衛星１０２を介して各家庭の受信設備（以降、ＡＶシステムともいう）１０３で受信される。衛星１０２には複数のトランスポンダが搭載されている。１つのトランスポンダは例えば３０Ｍｂｐｓの伝送能力を有している。各家庭のＡＶシステム１０３は、パラボラアンテナ１１１に接続されたＩＲＤ(Integrated Receiver Decorder)１１２と、このＩＲＤ１１２に接続されたモニタ装置１１４及びＭＤレコーダ／プレーヤ１とからなる。また、このＡＶシステム１０３は、ＩＲＤ１１２に対して操作を行うためのリモートコントローラ６４と、ＭＤレコーダ／プレーヤ１に対して操作を行うためのリモートコントローラ３２を備えている。

このＡＶシステム１０３では、パラボラアンテナ１１１で衛星１０２を介して放送されてきた信号が受信される。この受信信号がパラボラアンテナ１１１に取り付けられたＬＮＢ(Low Noize Block Down Converter)１１５で所定の周波数に変換され、ＩＲＤ１１２に供給される。

ＩＲＤ１１２における概略的な動作としては、受信信号から所定のチャンネルの信号を選局し、その選局された信号から番組としてのビデオデータ及びオーディオデータの復調を行ってビデオ信号、オーディオ信号として出力する。また、ＩＲＤ１１２では、番組としてのデータと共に多重化されて送信されてくる、ＧＵＩデータに基づいてＧＵＩ画面としての出力も行う。このようなＩＲＤ１１２の出力は、例えばモニタ装置１１４に対して供給される。これにより、モニタ装置１１４では、ＩＲＤ１１２により受信選局した番組の画像表示及び音声出力が行われ、また、ユーザの操作に従ってＧＵＩ画面を表示させることが可能となる。

ＭＤレコーダ／プレーヤ１は、装填されたミニディスクに対するオーディオデータの記録及び再生が可能な記録再生装置である。また、このＭＤレコーダ／プレーヤ１は、オーディオデータ（楽曲データ）及びこれに付随して関連付けされたアルバムジャケット等の静止画像データ（ピクチャファイル）、歌詞やライナーノーツ等のテキストデータ（テキストファイル）をディスクに記録し、かつ、記録されたこれらのピクチャファイル及びテキストファイル等のデータをオーディオデータの再生時間に同期させて再生出力することができるものである。

なお、上記オーディオデータに付随したピクチャファイル及びテキストファイル等のデータについては、後述するＭＤレコーダ／プレーヤ１での扱いに従って、便宜上「ＡＵＸデータ」ともいう。

ここで、このＡＶシステム１０３において、ＩＲＤ１１２及びＭＤレコーダ／プレーヤ１は、ＩＥＥＥ１３９４バス１１６によって相互接続されているものとされる。

つまり、ＡＶシステム１０３を構築しているＩＲＤ１１２及びＭＤレコーダ／プレーヤ１は、それぞれデータ伝送規格としてＩＥＥＥ１３９４に対応したデータインターフェイスを備えている。

これによって、このＡＶシステムでは、ＩＲＤ１１２にて受信された楽曲としてのオーディオデータ（ダウンロードデータ）を、ＡＴＲＡＣ方式により圧縮処理が施されたままの状態で直接取り込んで記録することができる。また、上記オーディオデータと共に送信側のサーバーから衛星にアップロードされるＡＵＸデータを、上記衛星からＩＲＤ１１２を介してＭＤレコーダにダウンロードして記録することも可能とされている。

ＩＲＤ１１２は、電話回線１０４を介して課金サーバ１０５と通信可能とされている。ＩＲＤ１１２には、各種情報が記憶されるＩＣカードが挿入されるようになっている。そして、例えば楽曲のオーディオデータのダウンロードが行われたとすると、これに関する履歴情報がＩＣカードに記憶される。このＩＣカードの情報は、電話回線１０４を介して所定の機会、タイミングで課金サーバ１０５に送られる。課金サーバ１０５は、この送られてきた履歴情報に従って金額を設定して課金処理を行い、ユーザに請求する。

これまでの説明から分かるように、本発明を適用したＡＶシステムを含むデジタル衛星放送システムでは、地上局１０１は、テレビ番組素材サーバ１０６からの音楽番組放送の素材となるビデオデータ及びオーディオデータと、楽曲素材サーバ１０７からのオーディオチャンネルの素材となるオーディオデータと、音声付加情報サーバ１０８からの音声データと、ＧＵＩデータサーバ１０９からのＧＵＩデータとを多重化して送信している。

そして、各家庭のＡＶシステム１０３でこの放送を受信すると、例えばモニタ装置１１４により、選局したチャンネルの番組を視聴することができる。また、番組のデータと共に送信されるＧＵＩデータを利用したＧＵＩ画面として、ＥＰＧ（Electrical Program Guide；電子番組ガイド）画面を表示させ、番組の検索等を行うことができる。また、例えば通常の番組放送以外の特定のサービス用のＧＵＩ画面を利用して所要の操作を行うことで、放送システムにおいて提供されている通常番組の視聴以外のサービスを享受することができる。

例えば、オーディオ（楽曲）データのダウンロードサービス用のＧＵＩ画面を表示させて、このＧＵＩ画面を利用して操作を行えば、ユーザが希望した楽曲のオーディオデータをダウンロードしてＭＤレコーダ／プレーヤ１によりディスクに記録して保存することが可能になる。

ここで、このデジタル衛星放送システムでは、地上局１０１から衛星１０２を介してのＡＶシステム１０３への送信を行うに当たり、ＤＳＭ－ＣＣ（デジタル蓄積メディア・コマンド・アンド・コントロール；Digital Strage Media-Command and Control）プロトコルを採用する。

ＤＳＭ－ＣＣ（ＭＰＥＧ－ｐａｒｔ６）方式は、既に知られているように、例えば、何らかのネットワークを介して、デジタル蓄積メディア（ＤＳＭ）に蓄積されたＭＰＥＧ符号化ビットストリームを取り出し(Retrieve)たり、或いはＤＳＭに対してストリームを蓄積(Store)するためのコマンドや制御方式を規定したものである。

そして、ＤＳＭ－ＣＣ方式によりデータ放送サービス（例えばＧ

ＵＩ画面など）のコンテンツ（オブジェクトの集合）を伝送するためには、コンテンツの記述形式を定義しておく必要がある。このデジタル衛星放送システムでは、コンテンツの記述形式の定義として先に述べたＭＨＥＧが採用されている。

このデジタル衛星放送システムにおける地上局１０１は、図２のように構成されている。

図２に示した地上局１０１において、テレビ番組素材登録システム１３１は、テレビ番組素材サーバ１０６から得られた素材データをＡＶサーバ１３５に登録する。この素材データはテレビ番組送出システム１３９に送られ、ここでビデオデータは例えばＭＰＥＧ２方式で圧縮され、オーディオデータは、例えばＭＰＥＧ２オーディオ方式によりパケット化される。テレビ番組送出システム１３９の出力はマルチプレクサ１４５に送られる。

また、楽曲素材登録システム１３２では、楽曲素材サーバ１０７からの素材データ、つまりオーディオデータを、ＭＰＥＧ２オーディオエンコーダ１３６Ａ、及びＡＴＲＡＣエンコーダ１３６Ｂに供給する。ＭＰＥＧ２オーディオエンコーダ１３６Ａ、ＡＴＲＡＣエンコーダ１３６Ｂでは、それぞれ供給されたオーディオデータについてエンコード処理（圧縮符号化）を行った後、ＭＰＥＧオーディオサーバ１４０Ａ及びＡＴＲＡＣオーディオサーバ１４０Ｂに登録させる。

ＭＰＥＧオーディオサーバ１４０Ａに登録されたＭＰＥＧオーディオデータは、ＭＰＥＧオーディオ送出システム１４３Ａに伝送されてここでパケット化された後、マルチプレクサ１４５に伝送される。ＡＴＲＡＣオーディオサーバ１４０Ｂに登録されたＡＴＲＡＣ

データは、ＡＴＲＡＣオーディオ送出システム１４３Ｂに４倍速ＡＴＲＡＣデータとして送られ、ここでパケット化されてマルチプレクサ１４５に送出される。

また、音声付加情報登録システム１３３では、音声付加情報サーバ１０８からの素材データである音声付加情報を音声付加情報データベース１３７に登録する。この音声付加情報データベース１３７に登録された音声付加情報は、音声付加情報送出システム１４１に伝送され、同様にして、ここでパケット化されてマルチプレクサ１４５に伝送される。

また、ＧＵＩ用素材登録システム１３４では、ＧＵＩデータサーバ１０９からの素材データであるＧＵＩデータを、ＧＵＩ素材データベース１３８に登録する。

ＧＵＩ素材データベース１３８に登録されたＧＵＩ素材データは、ＧＵＩオーサリングシステム１４２に伝送され、ここで、ＧＵＩ画面としての出力が可能なデータ形式となるように処理が施される。

つまり、ＧＵＩオーサリングシステム１４２に伝送されてくるデータとしては、例えば、楽曲のダウンロードのためのＧＵＩ画面であれば、アルバムジャケットの静止画像データ、歌詞などのテキストデータ、さらには、操作に応じて出力されるべき音声データなどである。

上記した各データはいわゆるモノメディアといわれるが、ＧＵＩオーサリングシステム１４２では、ＭＨＥＧオーサリングツールを用いて、これらのモノメディアデータを符号化して、これをオブジェクトとして扱うようにする。

そして、ＧＵＩ画面の表示態様と操作に応じた画像音声の出力態

様が得られるように上記オブジェクトの関係を規定したシナリオ記述ファイル（スクリプト）と共にＭＨＥＧ－５のコンテンツを作成する。

また、テレビ番組素材サーバ１０６の素材データを基とする画像・音声データ（ＭＰＥＧビデオデータ、ＭＰＥＧオーディオデータ）と、楽曲素材サーバ１０７の楽曲素材データを基とするＭＰＥＧオーディオデータ等も、ＧＵＩ画面に表示され、操作に応じた出力態様が与えられる。

従って、上記シナリオ記述ファイルとしては、上記ＧＵＩオーサリングシステム０４２では、上記したテレビ番組素材サーバ１０６の素材データを基とする画像・音声データ、楽曲素材サーバ１０７の楽曲素材データを基とするＭＰＥＧオーディオデータ、さらには、音声付加情報サーバ１０８を基とする音声付加情報も必要に応じてオブジェクトとして扱われて、ＭＨＥＧのスクリプトによる規定が行われる。

なお、ＧＵＩオーサリングシステム１４２から伝送されるＭＨＥＧコンテンツのデータとしては、スクリプトファイル、及びオブジェクトとしての各種静止画データファイルやテキストデータファイルなどとなるが、静止画データは、例えばＪＰＥＧ(Joint Photograph Experts Group)方式で圧縮された６４０×４８０ピクセルのデータとされ、テキストデータは例えば８００文字以内のファイルとされる。

ＧＵＩオーサリングシステム１４２にて得られたＭＨＥＧコンテンツのデータはＤＳＭ－ＣＣエンコーダ１４４に伝送される。

ＤＳＭ－ＣＣエンコーダ１４４では、ＭＰＥＧ２フォーマットに

従ったビデオ、オーディオデータのデータストリームに多重できる形式のトランスポートストリーム（以下ＴＳ(Transport Stream)とも略す）に変換して、パケット化されてマルチプレクサ１４５に出力される。

マルチプレクサ１４５においては、テレビ番組送出システム１３９からのビデオパケット及びオーディオパケットと、ＭＰＥＧオーディオ送出システム１４３Ａからのオーディオパケットと、ＡＴＲＡＣオーディオ送出システム１４３Ｂからの４倍速オーディオパケットと、音声付加情報送出システム１４１からの音声付加情報パケットと、ＧＵＩオーサリングシステム１４２からのＧＵＩデータパケットとが時間軸多重化されると共に、キー情報サーバ１１０から出力されたキー情報に基づいて暗号化される。

マルチプレクサ１４５の出力は電波送出システム１４６に伝送され、ここで例えば誤り訂正符号の付加、変調、及び周波数変換などの処理を施された後、アンテナから衛星１０２に向けて送信される。

図３は、地上局１０１から衛星１０２に送信出力される際のデータの一例を示している。なお、この図３に示す各データは実際には時間軸多重化されているものである。また、各データは、図３に示すように、時刻ｔ１から時刻ｔ２の間が１つのイベントとされ、時刻ｔ２から次のイベントとされる。ここでいうイベントとは、例えば音楽番組のチャンネルであれば、複数楽曲のラインナップの組を変更する単位であり、時間的には３０分或いは１時間程度となる。

図３に示すように、時刻ｔ１から時刻ｔ２のイベントでは、通常の動画の番組放送で、所定の内容Ａ１を有する番組が放送されている。また、時刻ｔ２から始めるイベントでは、内容Ａ２としての番

組が放送されている。この通常の番組で放送されているのは動画と音声である。

ＭＰＥＧオーディオチャンネル（１）～（１０）は、例えば、チャンネルＣＨ１からＣＨ１０の１０チャンネル分用意される。このとき、各オーディオチャンネルＣＨ１，ＣＨ２，ＣＨ３・・・ＣＨ１０では、１つのイベントが放送されている間は同一楽曲が繰り返し送信される。つまり、時刻ｔ１～ｔ２のイベントの期間においては、オーディオチャンネルＣＨ１では楽曲Ｂ１が繰り返し送信され、オーディオチャンネルＣＨ２では楽曲Ｃ１が繰り返し送信され、以下同様に、オーディオチャンネルＣＨ１０では楽曲Ｋ１が繰り返し送信されることになる。これは、その下に示されている４倍速ＡＴＲＡＣオーディオチャンネル（１）～（１０）についても共通である。

つまり、図３において、ＭＰＥＧオーディオチャンネルと４倍速ＡＴＲＡＣオーディオチャンネルのチャンネル番号である（）内の数字が同じものは同じ楽曲となる。また、音声付加情報のチャンネル番号である（）内の数字は、同じチャンネル番号を有するオーディオデータに付加されている音声付加情報である。更に、ＧＵＩデータとして伝送される静止画データやテキストデータも各チャンネルごとに形成されるものである。これらのデータは、図４Ａ～図４Ｄに示すようにＭＰＥＧ２のトランスポートパケット内で時分割多重されて送信され、図４Ｅ～図４Ｈに示すようにしてＩＲＤ１１２内では各データパケットのヘッダ情報を用いて再構築される。

図５は、本発明に係るデータ伝送システムの構成を示すブロック図である。

このデータ伝送システムは、上述のデジタル衛星放送システムに含まれたＡＶシステム１０３を構成するものであって、上記ＩＲＤ１１２として機能するデータ送信装置１０と上記ＭＤレコーダ／プレーヤ１として機能するデータ受信装置２０を備え、上記データ送信装置１０とデータ受信装置２０が伝送路３０を介して接続された構成となっている。

このデータ伝送システムにおいて、上記データ送信装置１０は、通信衛星から送られてくる衛星デジタル多チャネル放送番組を受信するセットトップボックスすなわち上述のＩＲＤ１１２であって、内部バス１１に接続された中央演算処理ユニット(CPU: Central Processing Unit)１２、メモリ１３、入力インターフェース１４、ユーザインターフェース１５、入出力インターフェース１６等により構成されている。上記入力インターフェース１４には衛星アンテナ１１５が接続されている。また、上記入出力インターフェース１６は、デジタルインターフェースであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス・インターフェース（以下、単にＩＥＥＥ１３９４インターフェースという）であって、ＩＥＥＥ１３９４バスからなる上記伝送路３０に接続されている。

このデータ送信装置１０において、上記ＣＰＵ１２は、上記メモリ１３に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェース１５を介して入力される操作情報に応じて番組の選局動作等の各種制御動作を行うようになっている。

そして、このデータ送信装置１０は、上記受信アンテナ１１５が接続された上記入力インターフェース１４により衛星デジタル多チ

ャネル放送信号の所望のチャンネルを選局して所望のチャンネルのコンテンツ（音楽データ）及びメタデータ（テキストデータやＪＰＥＧデータ等の関連データ）を受信し、受信した音楽データ及びメタデータ（関連データ）を上記入出力インターフェース１６から上記伝送路３０に送信する。

また、上記データ受信装置２０は、上記データ送信装置１０すなわちセットトップボックスにより受信したコンテンツ（音楽データ）及びメタデータ（関連データ）を磁気テープや光磁気ディスクなどの記録媒体を介して記録／再生する記録／再生装置であって、内部バス２１に接続された中央演算処理ユニット(CPU: Central Processing Unit)２２、メモリ２３、入出力インターフェース２４、ユーザインターフェース２５、メディアアクセス部２６等により構成されている。上記入出力インターフェース２４は、デジタルインターフェースであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス・インターフェース（以下、単にＩＥＥＥ１３９４インターフェースという）であって、ＩＥＥＥ１３９４バスからなる上記伝送路３０が接続されている。

図６は、上記伝送路３０として実際に用いられるＩＥＥＥ１３９４バスケーブルの構造例を示している。

この図６においては、コネクタ６００Ａと６００Ｂがケーブル６０１を介して接続されていると共に、ここでは、コネクタ６００Ａと６００Ｂのピン端子として、ピン番号１～６の６ピンが使用される場合を示している。

コネクタ６００Ａ，６００Ｂに設けられる各ピン端子については、

ピン番号１は電源（ＶＰ）、ピン番号２はグランド（ＶＧ）、ピン番号３はＴＰＢ１、ピン番号４はＴＰＢ２、ピン番号５はＴＰＡ１、ピン番号５はＴＰＡ２とされている。

そして、コネクタ６００Ａ－６００Ｂ間の各ピンの接続形態は、

ピン番号１（ＶＰ）－ピン番号１（ＶＰ）

ピン番号２（ＶＧ）－ピン番号２（ＶＧ）

ピン番号３（ＴＰＢ１）－ピン番号５（ＴＰＡ１）

ピン番号４（ＴＰＢ２）－ピン番号６（ＴＰＡ２）

ピン番号５（ＴＰＡ１）－ピン番号３（ＴＰＢ１）

ピン番号６（ＴＰＡ２）－ピン番号３（ＴＰＢ２）

のようになっている。そして、上記ピン接続の組のうち、

ピン番号３（ＴＰＢ１）－ピン番号５（ＴＰＡ１）

ピン番号４（ＴＰＢ２）－ピン番号６（ＴＰＡ２）

の２本のツイスト線の組により、差動で信号を相互伝送する信号線６０１Ａを形成し、

ピン番号５（ＴＰＡ１）－ピン番号３（ＴＰＢ１）

ピン番号６（ＴＰＡ２）－ピン番号３（ＴＰＢ２）

の２本のツイスト線の組により、差動で信号を相互伝送する信号線６０１Ｂを形成している。

上記２組の信号線６０１Ａ及び信号線６０１Ｂにより伝送される信号は、図７Ａに示すデータ信号(Data)と、図７Ｂに示すストローブ信号(Strobe)である。

図７Ａに示すデータ信号は、信号線６０１Ａ又は信号線６０１Ｂの一方を使用してＴＰＢ１，ＴＰＢ２から出力され、ＴＰＡ１，ＴＰＡ２に入力される。

また、図７Ｂに示すストローブ信号は、データ信号と、このデータ信号に同期する伝送クロックとについて所定の論理演算を行うことによって得られる信号であり、実際の伝送クロックよりは低い周波数を有する。このストローブ信号は、信号線６０１Ａ又は信号線６０１Ｂのうち、データ信号伝送に使用していない他方の信号線を使用して、ＴＰＡ１，ＴＰＡ２から出力され、ＴＰＢ１，ＴＰＢ２に入力される。

例えば、図７Ａ，図７Ｂに示すデータ信号及びストローブ信号が、或るＩＥＥＥ１３９４対応の機器に対して入力されたとすると、この機器においては、入力されたデータ信号とストローブ信号とについて所定の論理演算を行って、図７Ｃに示すような伝送クロック(Clock) を生成し、所要の入力データ信号処理に利用する。

ＩＥＥＥ１３９４規格では、このようなハードウェア的データ伝送形態を採ることで、高速な周期の伝送クロックをケーブルによって機器間で伝送する必要をなくし、信号伝送の信頼性を高めるようにしている。

なお、上記説明では６ピンの仕様について説明したが、ＩＥＥＥ１３９４フォーマットでは電源（ＶＰ）とグランド（ＶＧ）を省略して、２組のツイスト線である信号線６０１Ａ及び信号線６０１Ｂのみからなる４ピンの仕様も存在する。例えば、このＡＶシステム１０３におけるＭＤレコーダ／プレーヤ１では、実際には、この４ピン仕様のケーブルを用いることで、ユーザにとってより簡易なシステムを提供できるように配慮している。

ここで、ＩＥＥＥ１３９４規格では、ＩＥＥＥ１３９４バスを介して接続されたネットワーク内で行われる伝送動作をサブアクショ

ンと呼び、次の２種類のサブアクションが規定されている。すなわち、２つのサブアクションとして、「アシンクロナス(Asynchronous)データ転送」と呼ばれる通常のデータ伝送を行う非同期伝送モード、及び、「アイソクロナス(Isochronous) データ転送」と呼ばれる伝送帯域を保証した同期伝送モードが定義されている。

すなわち、ＩＥＥＥ１３９４規格では、図８に示すようにIsochronous cycle(nominal cycle)の周期を繰り返すことによって送信を行う。この場合、１Isochronous cycleは、１２５μｓｅｃとされ、帯域としては１００ＭＨｚに相当する。なお、Isochronous cycleの周期としては１２５μｓｅｃ以外とされても良いことが規定されている。そして、このIsochronous cycle 毎に、データをパケット化して送信する。

このIsochronous cycleの先頭には、１Isochronous cycleの開始を示すCycle Start Packetが配置される。

このCycle Start Packetは、Cycle Masterとして定義されたＩＥＥＥ１３９４ネットワークシステム内の特定の１機器によってその発生タイミングが指示される。

Cycle Start Packetに続いては、Isochronous Packetが優先的に配置される。Isochronous Packetは、図８のように、チャンネルごとにパケット化された上で時分割的に配列されて転送される(Isochronous subactions)。また、Isochronous subactions内においてパケット毎の区切りには、Isochronous gap といわれる休止区間（例えば０．０５μｓｅｃ）が設けられる。

このように、ＩＥＥＥ１３９４システムでは、１つの伝送線路によってIsochronous データをマルチチャンネルで送受信することが

可能とされている。

ここで、例えばこのＡＶシステムにおけるＭＤレコーダ／プレーヤ１が対応するＡＴＲＡＣデータ（圧縮オーディオデータ）をIsochronous 方式により送信することを考えた場合、ＡＴＲＡＣデータが１倍速の転送レート１．４Ｍｂｐｓであるとすれば、１２５μｓｅｃである１Isochronous cycle 周期ごとに、少なくともほぼ２０数MバイトのＡＴＲＡＣデータをIsochronous Packetとして伝送すれば、時系列的な連続性（リアルタイム性）が確保されることになる。

例えば、或る機器がＡＴＲＡＣデータを送信する際には、ＩＥＥＥ１３９４ネットワークシステム内のＩＲＭ(Isochronous Resource Manager)に対して、ＡＴＲＡＣデータのリアルタイム送信が確保できるだけの、Isochronous パケットのサイズを要求する。ＩＲＭでは、現在のデータ伝送状況を監視して許可／不許可を与え、許可が与えられれば、指定されたチャンネルによって、ＡＴＲＡＣデータをIsochronous Packetにパケット化して送信することができる。これがＩＥＥＥ１３９４インターフェイスにおける帯域予約といわれるものである。

Isochronous cycle の帯域内においてIsochronous subactionsが使用していない残りの帯域を用いて、Asynchronous subactions 、即ちAsynchronousのパケット送信が行われる。

図８では、Packet A, Packet B の２つのAsynchronous Packetが送信されている例が示されている。Asynchronous Packet の後には、ack gap(０．０５μｓｅｃ)の休止期間を挟んで、ＡＣＫ (Acknowledge) といわれる信号が付随する。ＡＣＫは、Asynchronous Trans

actionの過程において、何らかのAsynchronousデータの受信があったことを送信側(Controller)に知らせるためにハードウェア的に受信側(Target)から出力される信号である。

また、Asynchronous Packet 及びこれに続くＡＣＫからなるデータ伝送単位の前後には、１０μｓｅｃ程度のsubaction gap といわれる休止期間が設けられる。

ここで、Isochronous PacketによりＡＴＲＡＣデータを送信し、上記ＡＴＲＡＣデータに付随するＡＵＸデータファイルをAsynchronous Packet により送信するようにすれば、見かけ上、ＡＴＲＡＣデータとＡＵＸデータファイルとを同時に送信することが可能となる。

ここで、Asynchronous伝送は１対１のユニキャスト伝送であり、ブロードキャスト伝送を行うIsochronous 伝送に比べて盗聴が難しいという性質がある。

このデータ伝送システムでは、伝送帯域を確保できるIsochronous 伝送を用いて音楽データを伝送し、関連情報は、Asynchronous伝送を用いて伝送する。

そして、データ受信装置２０は、入出力インターフェース２４を介して音楽データと関連情報を受信し、それが記録可能であれば、メディアアクセス部２６により上記磁気テープや光磁気ディスクなどの記録媒体に記録する。

上記記録媒体に記録された音楽データと関連情報はメディアアクセス部２６により再生され、音楽データは、アナログ信号に変換されアナログ音声出力端子２６Ａから出力され、関連データは映像出力端子２６Ｂから出力される。また、上記メディアアクセス部２６

により再生され音楽データと関連情報は、ＩＥＥＥ１３９４インターフェースを介してさらに他の機器に伝送されることがある。

また、データ受信装置２０は、記録禁止の音楽データを受信した場合には、上記メディアアクセス部２６により記録媒体に記録することなく、単に音楽データをアナログ信号に変換してアナログ音声出力端子２６Ａから出力する。

このデータ受信装置２０において、上記ＣＰＵ２２は、上記メモリ２３に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェース２５を介して入力される操作情報に応じて、上記メディアアクセス部２６による記録動作等の各種制御動作を行うようになっている。

そして、このデータ伝送システムでは、受信アンテナ１１５を介してデータ送信装置１０により受信した所望のチャンネルのコンテンツ（音楽データ）及びメタデータ（関連データすなわちテキストデータやＪＰＥＧデータ等）を、それぞれ別の暗号方式、暗号鍵を用いて暗号化してデータ受信装置２０に伝送する。

すなわち、データ送信装置１０の要部構成を図９に示してあるように、上記データ送信装置１０の入力インターフェース１４は、衛星デジタル多チャネル放送信号の所望のチャンネルを選局するデマルチプレクサ(DEMUX) １４Ａと、このデマルチプレクサ(DEMUX) １４Ａにより選局された所望のチャンネルのトランスポートストリームを復号するデコーダ(DEC) １４Ｂを備え、また、入出力インターフェース１６は、上記デコーダ(DEC) １４Ｂにより復号された所望のチャンネルのトランスポートストリームに含まれているコンテンツ（音楽データ）及びメタデータ（関連データすなわちテキストデ

ータやＪＰＥＧデータ等）を分離するデータ分離回路１６Ａと、このデータ分離回路１６Ａにより分離されたコンテンツ（音楽データ）を暗号鍵Ｋiso により第１の暗号方式で暗号化してIsochronous Packetを生成する第１のエンコーダ１６Ｂと、上記データ分離回路１６Ａにより分離されたメタデータ（関連データ）を暗号鍵Ｋasync により第２の暗号方式で暗号化してAsynchronous Packet を生成する第１のエンコーダ１６Ｃを備える。

そして、上記データ送信装置１０における入出力インターフェース１６は、ＣＰＵ１２により制御されて、図１０のフローチャートに示すように動作する。すなわち、上記入出力インターフェース１６は、上記入力インターフェース１４を介して受信された所望のチャンネルのトランスポートストリームが入力されると（ステップＳ１）、入力されたトランスポートストリームに含まれているデータがコンテンツ（音楽データ）であるかメタデータ（関連データ）であるかを判定し（ステップＳ２）、コンテンツ（音楽データ）である場合には、そのコンテンツ（音楽データ）を暗号鍵Ｋiso により第１の暗号方式で暗号化し（ステップＳ３）、第１の暗号方式で暗号化したコンテンツ（音楽データ）をIsochronous Packetとして伝送する処理を行う（ステップＳ４）。また、入力されたトランスポートストリームに含まれているデータがメタデータ（関連データ）である場合には、そのメタデータ（関連データ）を暗号鍵ＫAsync により第２の暗号方式で暗号化し（ステップＳ５）、第２の暗号方式で暗号化したメタデータ（関連データ）をAsynchronous Packetとして伝送する処理を行う（ステップＳ６）。

このデータ伝送システムでは、上記データ伝送に先立って、デー

タ送信装置１０とデータ受信装置２０の間で相互認証と、Isochronous用とAsynchronous用の２種類の暗号鍵の共有プロトコルを実行する。具体的には、図１１のフローチャートに示すような認証・鍵共有プロトコルを実行してから、データ伝送を行う。なお、このデータ伝送システムにおけるデータ送信装置１０側の処理手順を図１２のフローチャートに示すとともに、データ受信装置２０側の処理手順を図１３のフローチャートに示す。

上記認証・鍵共有プロトコルを示す図１１では、データ送信装置１０をSource DeviceAで表し、データ受信装置２０をSink DeviceBで表す。これらの機器は、自分が正当であることを示す情報Ｋｖが機器の製造時に与えられ、秘密に保持している。

そして、このデータ伝送システムおいて、上記データ送信装置１０すなわちセットトップボックスのＣＰＵ１２は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース１６から上記伝送路３０を介してデータ受信装置２０に送信する（ステップＳ１０）。

上記データ受信装置２０すなわち記録装置のＣＰＵ２２は、上記入出力インターフェース２４に接続された上記伝送路３０を介して上記データ送信装置１０から送られてくるスタートコマンド(START command）を受信したら（ステップＳ２０）、認証・鍵共有プロトコルの開始要求(Request authentication)とｍ（例えばｍ＝６４）ビットの２つの乱数Ｂｎ１，Ｂｎ２を生成して上記データ送信装置１０に入出力インターフェース２４を介して送る（ステップＳ２１）。

上記データ送信装置１０のＣＰＵ１２は、上記入出力インターフ

ェース１６に接続された上記伝送路３０を介して上記データ受信装置２０から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)と乱数Ｂｎ１，Ｂｎ２を受信したら（ステップＳ１１）、ｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置１０に入出力インターフェース１６を介して送る（ステップＳ１２）。

上記データ受信装置２０は、上記データ送信装置１０から送られてくる２つの乱数Ａｎ１，Ａｎ２を受信する（ステップＳ２２）。

そして、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ２と上記ステップＳ１１で受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ２＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位ｍビットをレスポンスデータＲ２とし、このレスポンスデータＲ２を上記データ受信装置２０に入出力インターフェース１６を介して送る（ステップＳ１３）。図１１及び図１２の例では、ｍ＝６４ビットの例を示している。ここで、Ｘ‖Ｙは、ＸとＹとのビット連結を示す。なお、上記レスポンスデータＲ２を与える上記最上位ｍビットは、上記乱数のビット数ｍと同じビット数にしてあるが、上記乱数のビット数ｍと違っていてもよい。

上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０から送られてくるレスポンスデータＲ２を受信し（ステップＳ２３）、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２

で受信した乱数Ａｎ１と上記ステップＳ２１でデータ送信装置１０に送った乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ１＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

その出力の最上位ｍビットをレスポンスデータＲ１とし、このレスポンスデータＲ１を上記データ送信装置１０に入出力インターフェース２４を介して送る（ステップＳ２４）。図１１及び図１３の例では、ｍ＝６４ビットの例を示している。なお、上記レスポンスデータＲ１を与える上記最上位ｍビットも、上記乱数のビット数ｍと同じビット数にしてあるが、上記乱数のビット数ｍと違っていてもよい。

上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０から送られてくるレスポンスデータＲ１を受信する（ステップＳ１４）。

さらに、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ１と上記ステップＳ１１で受信した乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ’１＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

その出力の最上位ｍビットを参照データＲ’１ とする（ステップＳ１５）。すなわち、上記レスポンスデータＲ１と同じｍビットが参照データＲ’１ とされる 。

そして、上記データ送信装置１０のＣＰＵ１２は、上記参照データＲ’１ を上記ステップＳ１４で受信したレスポンスデータＲ１と比較する（ステップＳ１６）。このステップＳ１６において、レスポンスデータＲ１が参照データＲ’１ と一致しなければ、上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

上記ステップＳ１６においてレスポンスデータＲ１が参照データＲ’１ と一致した場合には、上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０を正当な機器であると判断し、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ１と上記ステップＳ１１で受信した乱数Ｂｎ１を連結した連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋiso ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位ｍビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵Ｋiso とする。また、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ２と上記ステップＳ１１で受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋasync＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位ｍビットをAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とする（ステップＳ１７）。

なお、上記２種類の暗号鍵Ｋiso , Ｋasync を与える上記最下位ｍビットも、上記乱数のビット数ｍと同じビット数にしてあるが、

上記乱数のビット数mと違っていてもよい。

一方、上記データ受信装置２０のＣＰＵ２２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２で受信した乱数Ａｎ２と上記ステップＳ２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ’２＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位mビットを参照データＲ’２ とする（ステップＳ２５）。すなわち、上記レスポンスデータＲ２と同じmビットが参照データＲ’２ とされる 。

そして、上記データ受信装置２０のＣＰＵ２２は、この参照データＲ’２ を上記ステップＳ２３で受信したレスポンスデータＲ２と比較する（ステップＳ２６）。このステップＳ２６において、レスポンスデータＲ２が参照データＲ’２ と一致しなければ、上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

また、上記ステップＳ２６においてレスポンスデータＲ２が参照データＲ’２ と一致した場合には、上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０を正当な機器であると判断し、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２で受信した乱数Ａｎ１と上記ステップＳ２１でデータ送信装置１０に送った乱数Ｂｎ１を連結した連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋ’iso ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位mビットをIsochronous 伝送で送られてくるデー

タを復号するために使用する暗号鍵K'isoとする。すなわち、上記暗号鍵Kisoと同じmビットが暗号鍵K'isoとされる 。

また、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２で受信した乱数Ａｎ２と上記ステップＳ２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２)をハッシュ関数Ｈａｓｈ［］に入力し、

K'async＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位mビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵K'asyncとする（ステップＳ２７）。すなわち、上記暗号鍵Kasync と同じmビットが暗号鍵K'asyncとされる 。

このデータ伝送システムでは、データ伝送に先立って、上記認証・鍵共有プロトコルをデータ送信装置１０とデータ受信装置２０の間でＩＥＥＥ１３９４のAsynchronous伝送によって実行することにより、データ送信装置１０とデータ受信装置２０が、相互に正当性を認証するとともに、Isochronous 伝送で暗号化したデータを送るための暗号鍵とAsynchronous伝送で暗号化したデータを送るための暗号鍵を共有することができる。

そして、このデータ伝送システムでは、上記認証・鍵共有プロトコルを実行した後に、データ送信装置１０から音楽データを暗号鍵Kiso で暗号化してIsochronous 伝送で送信し、また、関連データを暗号鍵Kasync で暗号化してAsynchronous伝送で送信し（ステップＳ１８）、データ受信装置２０は、Isochronous 伝送により送られてくる音楽データを暗号鍵K'isoで復号し、また、Asynchronous伝送で送られてくる関連データを暗号鍵K'asyncで復号する（ステ

ップＳ２８）。

すなわち、上記認証・鍵共有プロトコルの実行後は、データ受信装置２０は、データ送信装置１０からIsochronous 伝送により送られてくる音楽データを暗号鍵K'isoで復号し、また、Asynchronous伝送で送られてくる関連データを暗号鍵K'asyncで復号して、それぞれの平文データを得ることができる。

〔認証・鍵共有プロトコルの他の実施の形態〕

次に、このデータ伝送システムおいて、上記データ伝送に先立って実行する認証・鍵共有プロトコルの他の例を図１４のフローチャートに示す。この場合のデータ送信装置１０側の処理手順を図１５のフローチャートに示すとともに、データ受信装置２０側の処理手順を図１６のフローチャートに示す。

上記認証・鍵共有プロトコルを示す図１４では、データ送信装置１０をSource DeviceAで表し、データ受信装置２０をSink DeviceB で表す。これらの機器は、自分が正当であることを示す情報Ｋｖが機器の製造時に与えられ、秘密に保持している。

そして、このデータ伝送システムおいて、上記データ送信装置１０すなわちセットトップボックスのＣＰＵ１２は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース１６から上記伝送路３０を介してデータ受信装置２０に送信する（ステップＳ１１０）。

上記データ受信装置２０すなわち記録装置のＣＰＵ２２は、上記入出力インターフェース２４に接続された上記伝送路３０を介して上記データ送信装置１０から送られてくるスタートコマンド(START command）を受信したら（ステップＳ１２０）、認証・鍵共有プロ

トコルの開始要求(Request authentication)とｍ（例えばｍ＝６４）ビットの２つの乱数Ｂｎ１，Ｂｎ２を生成して上記データ送信装置１０に入出力インターフェース２４を介して送る（ステップＳ１２１）。

上記データ送信装置１０のＣＰＵ１２は、上記入出力インターフェース１６に接続された上記伝送路３０を介して上記データ受信装置２０から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)と乱数Ｂｎ１，Ｂｎ２を受信したら（ステップＳ１１１）、ｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置２０に入出力インターフェース１６を介して送る（ステップＳ１１２）。

上記データ受信装置２０は、上記データ送信装置１０から送られてくる２つの乱数Ａｎ１，Ａｎ２を受信する（ステップＳ１２２）。

そして、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１１２でデータ受信装置２０に送った乱数Ａｎ１と上記ステップＳ１１１で受信した乱数Ｂｎ１を連結した連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ’１ ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビット（例えばｐ＝６４）を参照データＲ’１とするとともに、

Ｋiso ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎ（例えばｎ＝６４）ビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵Ｋiso とする（ステップＳ１

１３）。ここで、Ｘ‖Ｙは、ＸとＹとのビット連結を示す。

そして、上記データ送信装置１０のＣＰＵ１２は、このようにして算出した暗号鍵Ｋiso と上記ステップＳ１１２でデータ受信装置２０に送った乱数Ａｎ２と上記ステップＳ１１１で受信した乱数Ｂｎ２を連結した連結データ(Ｋiso ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ(Ｋiso ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ[] に入力し、

Ｒ２＝Ｈａｓｈ［Ｋiso ‖Ａｎ２‖Ｂｎ２］msb_p

その出力の最上位ｐビットをレスポンスデータＲ２とする（ステップＳ１１４）。

そして、上記データ送信装置１０のＣＰＵ１２は、ステップＳ１１４で算出したレスポンスデータＲ２を上記データ受信装置２０に入出力インターフェース１６を介して送る（ステップＳ１１５）。

一方、上記データ受信装置２０のＣＰＵ２２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２２で受信した乱数Ａｎ１と上記ステップＳ１２１でデータ送信装置１０に送った乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ１　＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットをレスポンスデータＲ１とし、

K'iso＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵K'isoとする（ステップＳ１２３）。

また、上記データ受信装置２０のＣＰＵ２２は、このようにして

算出した暗号鍵K'isoと上記ステップＳ１２２で受信した乱数Ａｎ２と上記ステップＳ１２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ(Ｋｖ ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ'２ ＝Ｈａｓｈ［K'iso‖Ａｎ２‖Ｂｎ２］msb_p

その出力の最上位ｐビットを参照データＲ'２ とする（ステップＳ１２４）。

上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０から送られてくるレスポンスデータＲ２を受信し（ステップＳ１２５）、上記ステップＳ１２４で算出した参照Ｒ'２ と比較する（ステップＳ１２６）。このステップＳ１２６において、レスポンスデータＲ１が参照データＲ'１ と一致しなければ、上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

上記ステップＳ１２６においてレスポンスデータＲ２が参照データＲ'２ と一致した場合には、上記データ受信装置２０のＣＰＵ２２は、上記ステップＳ１２３で算出したレスポンスデータＲ１を上記データ送信装置１０に入出力インターフェース１６を介して送る（ステップＳ１２７）。

上記データ送信装置１０のＣＰＵ１０は、上記データ受信装置２０から送られてくるレスポンスデータＲ１を受信し（ステップＳ１１６）、上記ステップＳ１１３で算出した参照データＲ'１ と比較する（ステップＳ１１７）。このステップＳ１１７において、レスポンスデータＲ１が参照データＲ'１ と一致しなければ、上記デー

タ送信装置２０のＣＰＵ１２は、上記データ受信装置２０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

上記ステップＳ１１７においてレスポンスデータＲ１が参照データＲ'１ と一致した場合には、上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０を正当な機器であると判断し、上記ステップＳ１１３で算出した暗号鍵Ｋiso と上記ステップＳ１１２でデータ受信装置２０に送った乱数Ａｎ２と上記ステップＳ１１１で受信した乱数Ｂｎ２を連結した連結データ（Ｋiso ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ（Ｋiso ‖Ａｎ２‖Ｂｎ２)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋasync＝Ｈａｓｈ［Ｋiso ‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビット（例えばｑ＝６４）をAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とする（ステップＳ１１８）。

また、上記データ受信装置２０のＣＰＵ２２は、上記ステップＳ１２３で算出した暗号鍵Ｋ'isoと上記ステップＳ１２２で受信した乱数Ａｎ２と上記ステップＳ１２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ（Ｋ'iso‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（Ｋ'iso‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋ'async＝Ｈａｓｈ［Ｋ'iso‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵Ｋ'asyncとする（ステップＳ１２８）。

このデータ伝送システムでは、データ伝送に先立って、上記認証

・鍵共有プロトコルをデータ送信装置１０とデータ受信装置２０の間でＩＥＥＥ１３９４のAsynchronous伝送によって実行することにより、データ送信装置１０とデータ受信装置２０が、相互に正当性を認証するとともに、Isochronous 伝送で暗号化したデータを送るための暗号鍵とAsynchronous伝送で暗号化したデータを送るための暗号鍵を共有することができる。

すなわち、上記認証・鍵共有プロトコルの実行後は、データ送信装置１０から音楽データを暗号鍵Ｋiso で暗号化してIsochronous伝送で送信し、また、関連データを暗号鍵Ｋasync で暗号化してAsynchronous伝送で送信することによって（ステップＳ１１９）、データ受信装置２０は、Isochronous 伝送により送られてくる音楽データを暗号鍵Ｋ'isoで復号し、また、Asynchronous伝送で送られてくる関連データを暗号鍵Ｋ'asyncで復号することにより（ステップＳ１２９）、それぞれの平文データを得ることができる。

ここで、一般にIsochronous 伝送とAsynchronous伝送では性質が違うので、それぞれに用いられる暗号アルゴリズムやモードもそれぞれに適したものが使用される。そこで、Asynchronous伝送に使用される暗号アルゴリズムがIsochronous 伝送に使用されるものに比べて強度的に弱い場合、Asynchronous伝送に使用される暗号鍵Ｋasyncは、Isochronous 伝送に使用される暗号鍵Ｋisoに比べて比較的容易に露呈してしまうことになる。図１１に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報Ｋｖから暗号鍵Ｋasyncと暗号鍵Ｋisoを直接生成しているので、暗号鍵Ｋasyncが露呈してしまうと、例えば総当たり攻撃により情報Ｋｖが露呈してしまうことになる。

これに対して、図１４に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報Ｋｖから暗号鍵Ｋiso を生成し、この暗号鍵Ｋiso から暗号鍵Ｋasync を生成しているので、暗号鍵Ｋasync が露呈しても、攻撃者は、一方向性関数Ｈａｓｈを一度攻撃するだけでは情報Ｋｖを得ることはできず、総当たり攻撃により暗号鍵Ｋiso を求めて、しかる後に情報Ｋｖを総当たり攻撃しなければならない。

すなわち、図１４に示した認証・鍵共有プロトコルでは、図１１に示した認証・鍵共有プロトコルと比較して、各機器が秘密に保持している自分が正当であることを示す情報Ｋｖが露呈しにくく、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

なお、図１４に示した認証・鍵共有プロトコルでは、上述のデータ伝送システムでは、Isochronous 伝送に使用される暗号鍵Ｋiso に基づいて、Asynchronous伝送に使用される暗号鍵Ｋasync を生成するようにしたが、逆に、Asynchronous伝送に使用される暗号鍵Ｋasync を情報Ｋｖ，乱数Ａｎ１，乱数Ｂｎ１から生成し、生成された暗号鍵Ｋasync、乱数Ａｎ２，乱数Ｂｎ２から Isochronous 伝送に使用される暗号鍵Ｋisoを生成するように構成しても良い。

また、図１４に示した認証・鍵共有プロトコルでは、データ送信装置１０で暗号鍵Ｋiso から生成したデータをレスポンスデータＲ２としてデータ受信装置２０に送信し、データ受信装置２０で情報Ｋｖから生成したデータをレスポンスデータＲ１としてデータ送信装置１０に送信するように構成したが、データ送信装置１０が情報Ｋｖから生成したデータをレスポンスデータＲ２としてデータ受信

装置２０に送信し、データ受信装置２０が暗号鍵Ｋiso から生成したデータをレスポンスデータＲ１としてデータ送信装置１０に送信するように構成しても良い。

なお、上述のデータ伝送システムでは、各認証・鍵共有プロトコルを実行することによりデータ送信装置１０とデータ受信装置２０の間で共有される暗号鍵Ｋiso，K'iso 及び暗号鍵Ｋasync，K'async を用いて伝送データを暗号化／復号するようにしているが、実際に伝送するデータを暗号化／復号するための暗号鍵（コンテンツキー）は別に用意して、暗号鍵Ｋiso，K'iso 及び暗号鍵Ｋasync，K'asyncを用いてコンテンツキーをデータ送信装置１０とデータ受信装置２０の間で共有することもできる。

以上のように本実施の形態では、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで伝送し、上記データに関する関連データを第２の伝送モードで伝送するので、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の２種類の伝送方式を採用して、データを確実に伝送することができる。

また、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで伝送し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで伝送するにより、伝送帯域の保証が必要なデータと上記データに関する関連データを安全に伝送することができる。

さらに、データ伝送に先立って、データ送信装置とデータ受信装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコル

を実行することによって、データ送信装置とデータ受信装置が互いの正当性を認証するとともに、暗号鍵を共有することができ、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

請求の範囲

１．　伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記インターフェースを介して送信する送信制御手段とを備える第１の情報処理装置と、

伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記インターフェースを介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する受信制御手段とを備える第２の情報処理装置と

を具備する情報処理システム。

２．　データ伝送に先立って、上記第１の情報処理装置と第２の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第１項記載の情報処理システム。

３．　音楽データを上記第１の伝送モードで伝送し、上記音楽データに関する関連データを第２の伝送モードで伝送する請求の範囲第１項記載の情報処理システム。

４．　上記第１の情報処理装置と第２の情報処理装置をＩＥＥＥ(T

he International of Electrical and Electronics Engineers,Inc.）１３９４規格に準拠したインターフェースを介して接続し、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで伝送する請求の範囲第１項記載の情報処理システム。

５．　データ伝送に先立って、上記第１の情報処理装置と第２の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する請求の範囲第４項記載の情報処理システム。

６．　上記第２の情報処理装置は、２つの乱数を生成して第１の情報処理装置に送信し、

上記第１の情報処理装置は、２つの乱数を生成して上記第２の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第１項の情報処理システム。

７．　上記第１の情報処理装置は、自分が正当な機器であることを

示す情報と上記生成した乱数と受信した乱数とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第６項記載の情報処理システム。

８．　上記第２の情報処理装置は、２つの乱数Ｒ１，Ｒ２を生成して第１の情報処理装置に送信し、

上記第１の情報処理装置は、２つの乱数Ｓ１，Ｓ２を生成して上記第２の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す

情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１とに基づいて生成したデータＱ’　が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２とに基づいて生成したデータＰ’　が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第７項記載の情報処理システム。

９．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を用いて一方向関数を演算した結果を用いて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を用いて一方向関数を演算した結果を用いて、上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を用いて一方向関

数を演算した結果を用いて、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を用いて一方向関数を演算した結果を用いて、上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第８項記載の情報処理システム。

１０．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を用いて一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を用いて一方向関数を演算した結果を用いて生成したデータＱを上記第２の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を用いて一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を用いて一方向関数を演算した結果を用いて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで

送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第９項記載の情報処理システム。

１１．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第９項記載の情報処理システム。

１２．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第１１項記載の情報処理システム。

１３．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第１１項記載の情報処理システム。

１４．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の最上位ｍビットを用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第１３項記載の情報処理システム。

１５．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて、上記第２の伝送モード

で送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて、上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第８項記載の情報処理システム。

１６．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第１５項記載の情報処理システム。

１７．　上記第１の情報処理装置及び上記第２の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、生成された暗号鍵と上記生成した乱数と受信した乱数とに基づいて、他方の伝送モードの暗号鍵を生成する請求の範囲第６項記載の情報処理システム。

１８．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第１の

伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータＰ’が受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱを上記第１の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成する請求の範囲第１７項記載の情報処理システム。

１９．　上記第２の情報処理装置は、２つの乱数Ｒ１，Ｒ２を生成して第１の情報処理装置に送信し、

上記第１の情報処理装置は、２つの乱数Ｓ１，Ｓ２を生成して上記第２の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す

情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵Ｋ１を生成すると共に、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵Ｋ１’を生成すると共に、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２とに基づいて生成したデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて生成したデータＱを上記第１の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵Ｋ２’を生成し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、既に生成

されている伝送モード用の暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵Ｋ２を生成する請求の範囲第１８項記載の情報処理システム。

２０．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ１を生成すると共に、生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ１’を生成すると共に、生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ２’を生成する請求の範囲第１９項記載の情報処理システム。

２１．　上記第１の情報処理装置は、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２とを用いて一方向関数を演算した結果を用いてデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とを用いて一方

向関数を演算した結果を用いて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とを用いて一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、暗号鍵Ｋ２を生成する請求の範囲第２０項記載の情報処理システム。

２２．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第２０項記載の情報処理システム。

２３．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第２２項記載の情報処理システム。

２４．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第２２項記載の情報処理システム。

２５．　上記第１の情報処理装置及び上記第２の情報処理装置は、一方向関数を演算した結果の最上位ｍビットを用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第２４項記載の情報処理システム。

２６．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１を連結した

連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ１を生成すると共に、生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ１’を生成すると共に、生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ２’を生成する請求の範囲第１９項記載の情報処理システム。

２７．　上記第１の情報処理装置は、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いてデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱ

’が受信したデータＱと一致した場合には、暗号鍵Ｋ２を生成する請求の範囲第２６項記載の情報処理システム。

２８．　第１の情報処理装置と第２の情報処理装置との間で伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介してデータ伝送を行う情報処理方法であって、

上記第１の情報処理装置から伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで送信するとともに、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで送信し、

上記第２の情報処理装置側で第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する情報処理方法

２９．　データ伝送に先立って、上記第１の情報処理装置と第２の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第２８項記載の情報処理方法。

３０．　音楽データを上記第１の伝送モードで伝送し、上記音楽データに関する関連データを第２の伝送モードで伝送する請求の範囲第２８項記載の情報処理方法。

３１．　上記第１の情報処理装置と第２の情報処理装置との間で、をＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを介して、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous)伝送モードで伝送し、上記データに関する関連データをアシンクロナ

ス(Asynchronous)伝送モードで伝送する請求の範囲第２８項記載の情報処理方法。

３２．　データ伝送に先立って、上記第１の情報処理装置と第２の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する請求の範囲第３１項記載の情報処理方法。

３３．　上記第２の情報処理装置は、２つの乱数を生成して第１の情報処理装置に送信し、

上記第１の情報処理装置は、２つの乱数を生成して上記第２の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第２８項の情報処理方法。

３４．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデー

タＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第３３項記載の情報処理方法。

３５．　上記第２の情報処理装置は、２つの乱数Ｒ１，Ｒ２を生成して第１の情報処理装置に送信し、

上記第１の情報処理装置は、２つの乱数Ｓ１，Ｓ２を生成して上記第２の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１とに基づいて生成

したデータＱ’　が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２とに基づいて生成したデータＰ’　が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第３４項記載の情報処理方法。

３６．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を用いて一方向関数を演算した結果を用いて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を用いて一方向関数を演算した結果を用いて、上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を用いて一方向関数を演算した結果を用いて、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を用いて一方向関数を演算した結果を用いて、上記

第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第３５項記載の情報処理方法。

３７．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を用いて一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を用いて一方向関数を演算した結果を用いて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を用いて一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を用いて一方向関数を演算した結果を用いて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第３６項記載の情報処理方法。

３８．　上記第１の情報処理装置及び上記第２の情報処理装置において一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ

１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第３６項記載の情報処理方法。

３９．　上記第１の情報処理装置及び上記第２の情報処理装置において、一方向関数を演算した結果の一部のビット値を用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第３８項記載の情報処理方法。

４０．　上記第１の情報処理装置及び上記第２の情報処理装置において、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第３８項記載の情報処理方法。

４１．　上記第１の情報処理装置及び上記第２の情報処理装置において、一方向関数を演算した結果の最上位ｍビットを用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第４０項記載の情報処理方法。

４２．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて、上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて、上記第１の伝送

モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて、上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第３５項記載の情報処理方法。

４３．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モード

で送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第４２項記載の情報処理方法。

４４．　上記第１の情報処理装置及び上記第２の情報処理装置において、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、生成された暗号鍵と上記生成した乱数と受信した乱数とに基づいて、他方の伝送モードの暗号鍵を生成する請求の範囲第３３項記載の情報処理方法。

４５．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータＰ’が受信したデータＰとが一致するか否かを検証し、

一致した場合には、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱを上記第１の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成する請求の範囲第４４項記載の情報処理方法。

４６．　上記第２の情報処理装置は、２つの乱数Ｒ１，Ｒ２を生成して第１の情報処理装置に送信し、

上記第１の情報処理装置は、２つの乱数Ｓ１，Ｓ２を生成して上記第２の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵Ｋ１を生成すると共に、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数

Ｓ２とに基づいて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵Ｋ１’を生成すると共に、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２とに基づいて生成したデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて生成したデータＱを上記第１の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵Ｋ２’を生成し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、既に生成されている伝送モード用の暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵Ｋ２を生成する請求の範囲第４５項記載の情報処理方法。

４７．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ１を生成すると共に、生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ１’を生成すると共に、生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ２’を生成する請求の範囲第４６項記載の情報処理方法。

４８．　上記第１の情報処理装置は、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２とを用いて一方向関数を演算した結果を用いてデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とを用いて一方向関数を演算した結果を用いて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とを用いて一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータ

Ｑと一致した場合には、暗号鍵Ｋ２を生成する請求の範囲第４７項記載の情報処理方法。

４９．　上記第１の情報処理装置及び上記第２の情報処理装置において、一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第４７項記載の情報処理方法。

５０．　上記第１の情報処理装置及び上記第２の情報処理装置において、一方向関数を演算した結果の一部のビット値を用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第４９項記載の情報処理方法。

５１．　上記第１の情報処理装置及び上記第２の情報処理装置において、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ１、暗号鍵Ｋ２、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第４９項記載の情報処理方法。

５２．　上記第１の情報処理装置及び上記第２の情報処理装置において、一方向関数を演算した結果の最上位ｍビットを用いてデータＰ、データＱ’、データＱ及びデータＰ’を生成する請求の範囲第５１項記載の情報処理方法。

５３．　上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ１を生成すると共に、生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ２を生成し、

上記第２の情報処理装置は、自分が正当な機器であることを示す

情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ１’を生成すると共に、生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ２’を生成する請求の範囲第４６項記載の情報処理方法。

５４．　上記第１の情報処理装置は、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを上記第２の情報処理装置に送信し、

上記第２の情報処理装置は、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いてデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱを上記第１の情報処理装置に送信し、

上記第１の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、暗号鍵Ｋ２を生成する請求の範囲第５３項記載の情報処理方法。

５５．　伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝

送モードで上記インターフェースを介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記インターフェースを介して送信する送信制御手段とを備える情報処理装置。

５６．　上記送信制御手段は、データ伝送に先立って、他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第５５項記載の情報処理装置。

５７．　上記送信制御手段は、音楽データを上記第１の伝送モードで伝送し、上記音楽データに関する関連データを第２の伝送モードで伝送する請求の範囲第５５項記載の情報処理装置。

５８．　上記インターフェースとしてＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを有し、上記送信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで伝送する請求の範囲第５５項記載の情報処理装置。

５９．　上記送信制御手段は、データ伝送に先立って、他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する請求の範囲第５８項記載の情報処理装置。

６０．　上記送信制御手段は、２つの乱数を生成して他の情報処理装置に送信して、上記他の情報処理装置が生成した２つの乱数を受信し、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第１の伝送モードで送信するデータを

暗号化するために使用する暗号鍵及び第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成する請求の範囲第５５項の情報処理装置。

６１．　上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱを受信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成する請求の範囲第６０項記載の情報処理装置。

６２．　上記送信制御手段は、上記他の情報処理装置が生成した乱数Ｒ２を受信し、２つの乱数Ｓ１，Ｓ２を生成して上記他の情報処理装置に送信するとともに、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２とに基づいて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数Ｓ１と生成した乱数Ｒ１とに基づいて生成したデータＱを受信し、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送

信するデータを暗号化するために使用する暗号鍵Ｋ２を生成する請求の範囲第６１項記載の情報処理装置。

６３．　上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を用いて一方向関数を演算した結果を用いて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を用いて一方向関数を演算した結果を用いて、上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成する請求の範囲第６２項記載の情報処理装置。

６４．　上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を用いて一方向関数を演算した結果を用いて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を用いて一方向関数を演算した結果を用いて生成したデータＱを受信し、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を用いて一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成する請求の範囲第６３項記載の情報処理装置。

６５．　上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ１及び暗号鍵Ｋ２を生成する請求の範囲

第６３項記載の情報処理装置。

６６．　上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いてデータＰ及びデータＱ’を生成する請求の範囲第６５項記載の情報処理装置。

６７．　上記送信制御手段は、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ１及び暗号鍵Ｋ２を生成する請求の範囲第６５項記載の情報処理装置。

６８．　上記送信制御手段は、一方向関数を演算した結果の最上位ｍビットを用いてデータＰ及びデータＱ’を生成する請求の範囲第６７項記載の情報処理装置。

６９．　上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて、上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成する請求の範囲第６２項記載の情報処理装置。

７０．　上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した

結果を用いて生成したデータＱを受信し、自分が正当な機器であることを示す情報と上記生成した乱数Ｓ１と受信した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ１及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵Ｋ２を生成する請求の範囲第６９項記載の情報処理装置。

７１．　上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、生成された暗号鍵と上記生成した乱数と受信した乱数とに基づいて、他方の伝送モードの暗号鍵を生成する請求の範囲第６０項記載の情報処理装置。

７２．　上記送信制御手段は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱを受信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数

とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成する請求の範囲第７１項記載の情報処理装置。

７３．　上記送信制御手段は、上記他の情報処理装置が生成した２つの乱数Ｒ１，Ｒ２を受信し、２つの乱数Ｓ１，Ｓ２を生成して上記他の情報処理装置に送信するとともに、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵Ｋ１を生成すると共に、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とに基づいて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて生成したデータＱを受信し、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とに基づいて生成したデータＱ’が受信したデータＱと一致した場合には、既に生成されている伝送モード用の暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵Ｋ２を生成する請求の範囲第７２項記載の情報処理装置。

７４．　上記送信制御手段は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ１を生成すると共に、生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ２を生成する請求の範囲第７３項記載の情報処理装置。

７５．　上記送信制御手段は、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とを用いて一方向関数を演算した結果を用いて生成したデータＱを受信し、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とを用いて一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、暗号鍵Ｋ２を生成する請求の範囲第７４項記載の情報処理装置。

７６．　上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ１及び暗号鍵Ｋ２を生成する請求の範囲第７４項記載の情報処理装置。

７７．　上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いてデータＰ及びデータＱ’を生成する請求の範囲第７６項記載の情報処理装置。

７８．　上記送信制御手段は、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ１及び暗号鍵Ｋ２を生成する請求の範囲第７６項記載の情報処理装置。

７９．　上記送信制御手段は、一方向関数を演算した結果の最上位ｍビットを用いてデータＰ及びデータＱ’を生成する請求の範囲第７８項記載の情報処理装置。

８０．　上記送信制御手段は、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ１を生成すると共に、生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ２を生成する請求の範囲第７３項記載の情報処理装置。

８１．　上記送信制御手段は、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱを受信し、自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱ’が受信したデータＱと一致した場合には、暗号鍵Ｋ２を生成する請求の範囲第８０項記載の情報処理装置。

８２．　伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記インターフ

ェースを介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する受信制御手段とを備える情報処理装置。

８３．　上記受信制御手段は、データ伝送に先立って、他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第８２項記載の情報処理装置。

８４．　上記受信制御手段は、音楽データを上記第１の伝送モードで受信し、上記音楽データに関する関連データを第２の伝送モードで受信する請求の範囲第８２項記載の情報処理装置。

８５．　上記インターフェースとしてＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを有し、上記受信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous) 伝送モードで受信し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで受信する請求の範囲第８２項記載の情報処理装置。

８６．　上記受信制御手段は、データ伝送に先立って、上記他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する請求の範囲第８５項記載の情報処理装置。

８７．　上記受信制御手段は、２つの乱数を生成して他の情報処理装置に送信して、上記他の情報処理装置が生成した２つの乱数を受信し、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範

囲第８２項の情報処理装置。

８８．　上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と生成した乱数と受信した乱数とに基づいて生成したデータＰを受信して、

自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱを上記他の情報処理装置に送信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第８７項記載の情報処理装置。

８９．　上記受信制御手段は、２つの乱数Ｒ１，Ｒ２を生成して他の情報処理装置に送信して、上記他の情報処理装置が生成した２つの乱数Ｓ１，Ｓ２を受信するとともに、上記他の情報処理装置が自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２とに基づいて生成したデータＰを受信し、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて生成したデータＱを上記他の情報処理装置に送信するとともに、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２とに基づいて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第８８項記載の情報処理装置。

９０．　上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を用いて一方向関数を演算した結果を用いて、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を用いて一方向関数を演算した結果を用いて、上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第８９項記載の情報処理装置。

９１．　上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を用いて一方向関数を演算した結果を用いて生成したデータＰを受信し、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を用いて一方向関数を演算した結果を用いて生成したデータＱを上記他の情報処理装置に送信し、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を用いて一方向関数を演算した結果を用いて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第９０項記載の情報処理装置。

９２．　上記受信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第９０項記載の情報処理装置。

９３．　上記受信制御手段は、一方向関数を演算した結果の一部の

ビット値を用いてデータＱ及びデータＰ’を生成する請求の範囲第９２項記載の情報処理装置。

９４．　上記受信制御手段は、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第９２項記載の情報処理装置。

９５．　上記受信制御手段は、一方向関数を演算した結果の最上位ｍビットを用いてデータＱ及びデータＰ’を生成する請求の範囲第９４項記載の情報処理装置。

９６．　上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて、上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第８９項記載の情報処理装置。

９７．　上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と上記生成した乱数Ｓ２と受信した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを受信し、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱを上記他の情報処理装置に送信し、自分が正当な機器であることを示す情報と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結し

た連結データに対して一方向関数を演算した結果を用いて生成したデータＰ’が受信したデータＰと一致した場合には、上記第１の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’１及び上記第２の伝送モードで送信されるデータを復号するために使用する暗号鍵Ｋ’２を生成する請求の範囲第９６項記載の情報処理装置。

９８．　上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータＰを受信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータＰ’が受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータＱを上記他の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝

送モードの暗号鍵を生成する請求の範囲第８７項記載の情報処理装置。

９９．　上記受信制御手段は、２つの乱数Ｒ１，Ｒ２を生成して他の情報処理装置に送信し、上記他の情報処理装置が生成した２つの乱数Ｓ１，Ｓ２を受信するとともに、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数Ｒ１と上記生成した乱数Ｓ１とに基づいて、上記第１の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第２の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵Ｋ１を生成すると共に、上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とに基づいて生成したデータＰを受信し、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて、上記第１の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵Ｋ１’を生成すると共に、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２とに基づいて生成したデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とに基づいて生成したデータＱを上記他の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２とに基づいて、上記第１の伝送モード及び上記第２の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵Ｋ２’を生

成する請求の範囲第９８項記載の情報処理装置。

１００．　上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ１’を生成すると共に、生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて暗号鍵Ｋ２’を生成する請求の範囲第９９項記載の情報処理装置。

１０１．　上記受信制御手段は、上記他の情報処理装置が上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２とを用いて一方向関数を演算した結果を用いて生成したデータＰを受信し、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２とを用いて一方向関数を演算した結果を用いてデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１とを用いて一方向関数を演算した結果を用いて生成したデータＱを上記他の情報処理装置に送信する請求の範囲第１００項記載の情報処理装置。

１０２．　上記受信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請求の範囲第１００項記載の情報処理装置。

１０３．　上記受信制御手段は、一方向関数を演算した結果の一部のビット値を用いてデータＱ及びデータＰ’を生成する請求の範囲第１０２項記載の情報処理装置。

１０４．　上記受信制御手段は、一方向関数を演算した結果の最下位ｎビットを用いて、暗号鍵Ｋ’１及び暗号鍵Ｋ’２を生成する請

求の範囲第１０２項記載の情報処理装置。

１０５．　上記受信制御手段は、一方向関数を演算した結果の最上位ｍビットを用いてデータＱ及びデータＰ’を生成する請求の範囲第１０４項記載の情報処理装置。

１０６．　上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ１’を生成すると共に、生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵Ｋ２’を生成する請求の範囲第９９項記載の情報処理装置。

１０７．　上記受信制御手段は、上記他の情報処理装置が上記生成された暗号鍵Ｋ１と受信した乱数Ｒ２と上記生成した乱数Ｓ２を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＰを受信し、上記生成された暗号鍵Ｋ１’と受信した乱数Ｓ２と上記生成した乱数Ｒ２を連結した連結データに対して一方向関数を演算した結果を用いてデータＰ’と受信したデータＰとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数Ｓ１と上記生成した乱数Ｒ１を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータＱを上記他の情報処理装置に送信する請求の範囲第１０６項記載の情報処理装置。

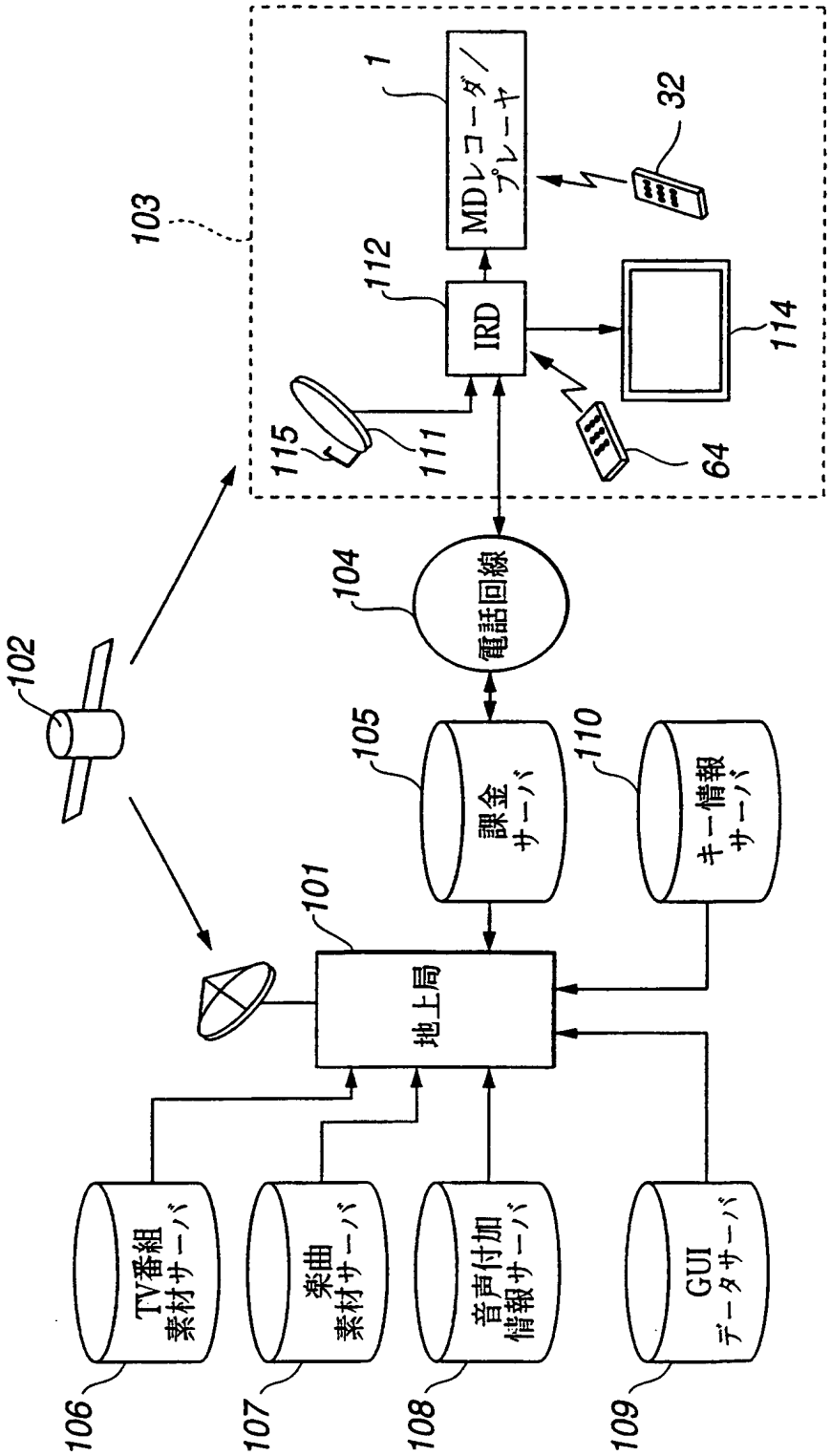

103
1
MDレコーダ／プレーヤ
32
112
IRD
114
115
111
64
104
電話回線
102
105
課金サーバ
110
キー情報サーバ
101
地上局
106
TV番組素材サーバ
107
楽曲素材サーバ
108
音声付加情報サーバ
109
GUIデータサーバ

FIG.1

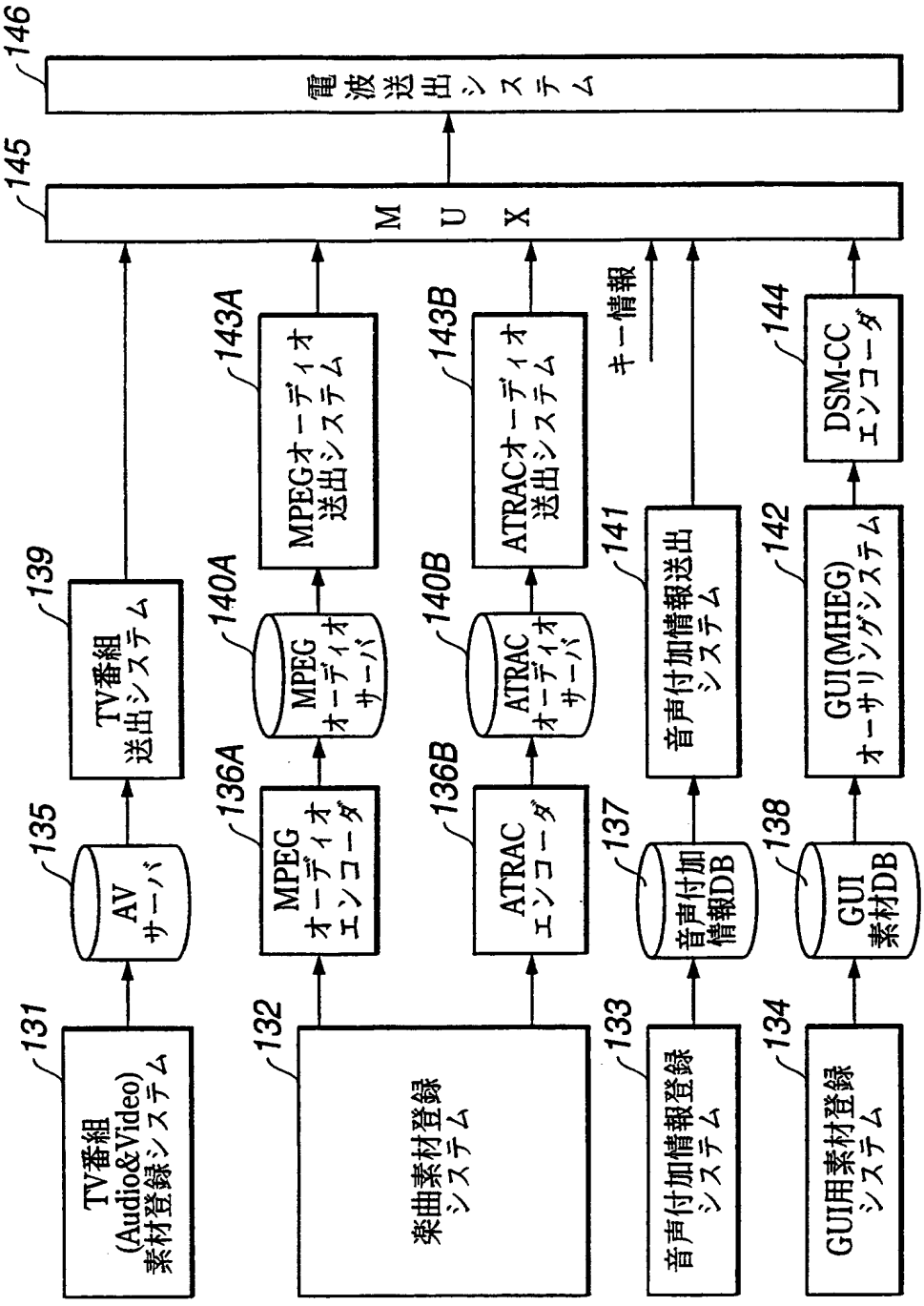

146
電波送出システム
145
M U X
キー情報
131
TV番組 (Audio&Video) 素材登録システム
135
AV サーバ
139
TV番組 送出システム
132
楽曲素材登録システム
136A
MPEG オーディオ エンコーダ
140A
MPEG オーディオ サーバ
143A
MPEGオーディオ 送出システム
136B
ATRAC エンコーダ
140B
ATRAC オーディオ サーバ
143B
ATRACオーディオ 送出システム
133
音声付加情報登録システム
137
音声付加 情報DB
141
音声付加情報送出 システム
134
GUI用素材登録システム
138
GUI 素材DB
142
GUI(MHEG) オーサリングシステム
144
DSM-CC エンコーダ

FIG.2

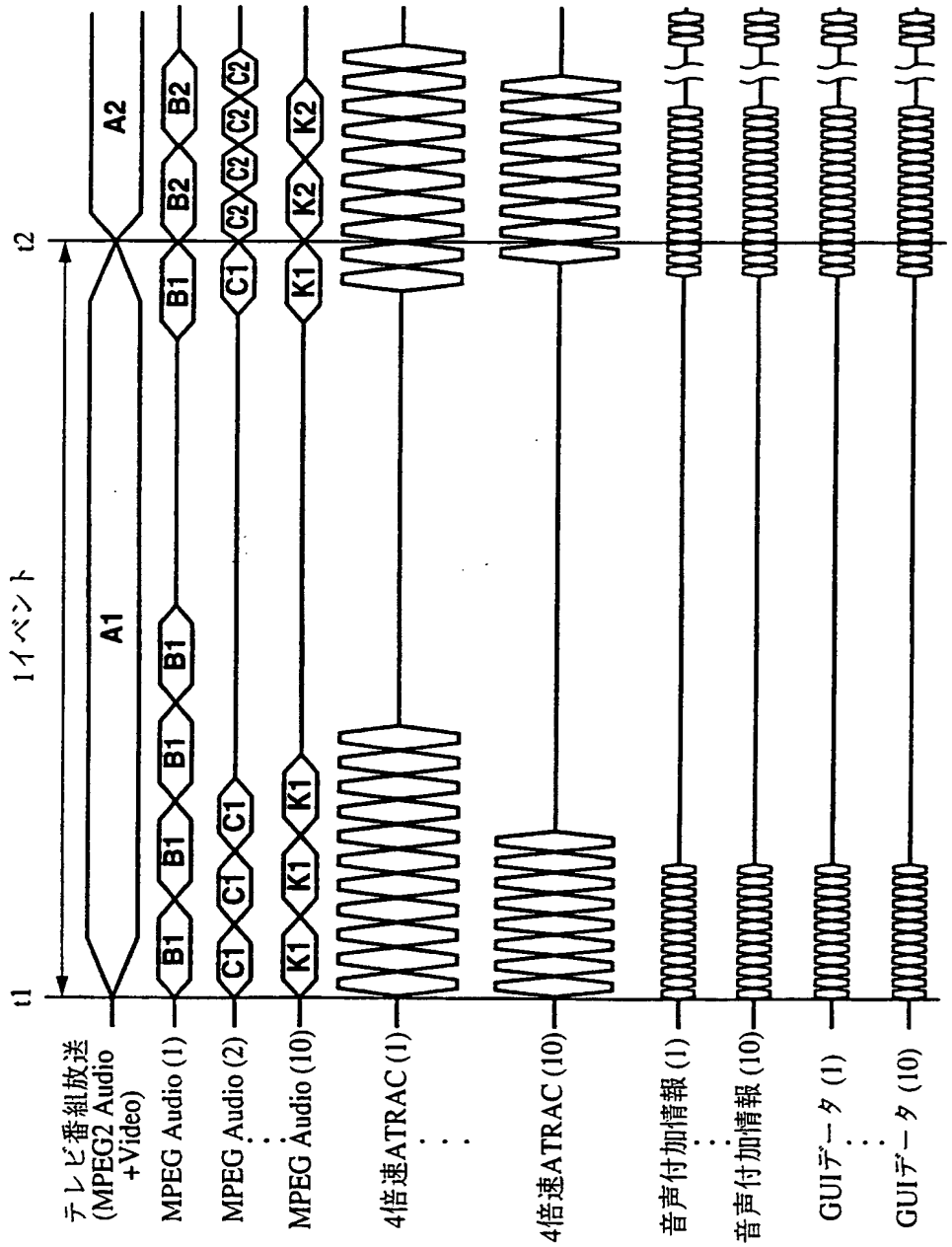

t1
t2
1イベント
テレビ番組放送 (MPEG2 Audio +Video)
MPEG Audio (1)
MPEG Audio (2)
MPEG Audio (10)
4倍速ATRAC (1)
4倍速ATRAC (10)
音声付加情報 (1)
音声付加情報 (10)
GUIデータ (1)
GUIデータ (10)
A1
A2
B1
B2
C1
C2
K1
K2

FIG.3

FIG.4A

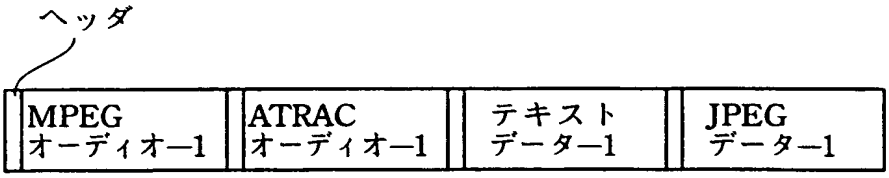


FIG.4B

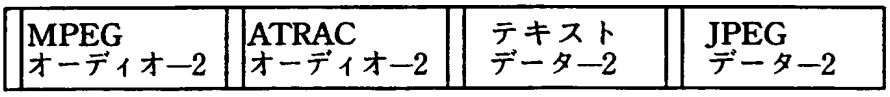


FIG.4C

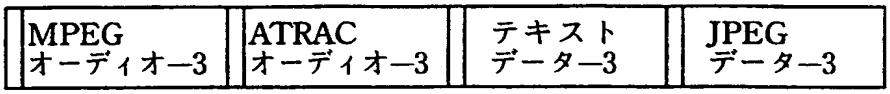


FIG.4D

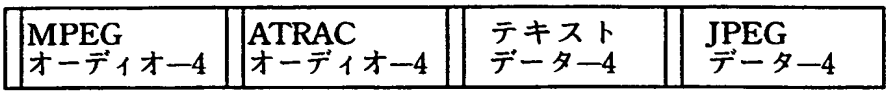


FIG.4E

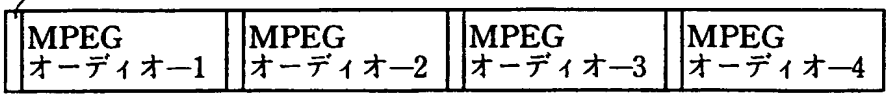


FIG.4F

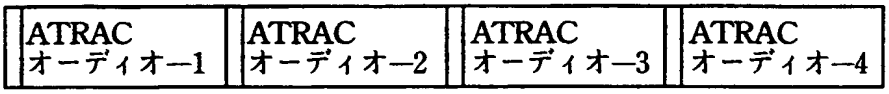


FIG.4G

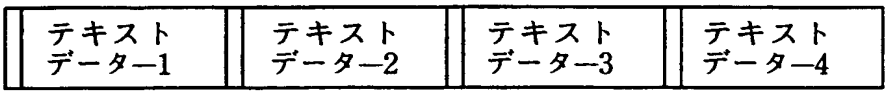
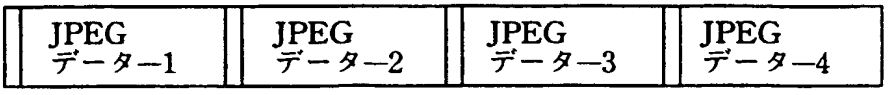


FIG.4H



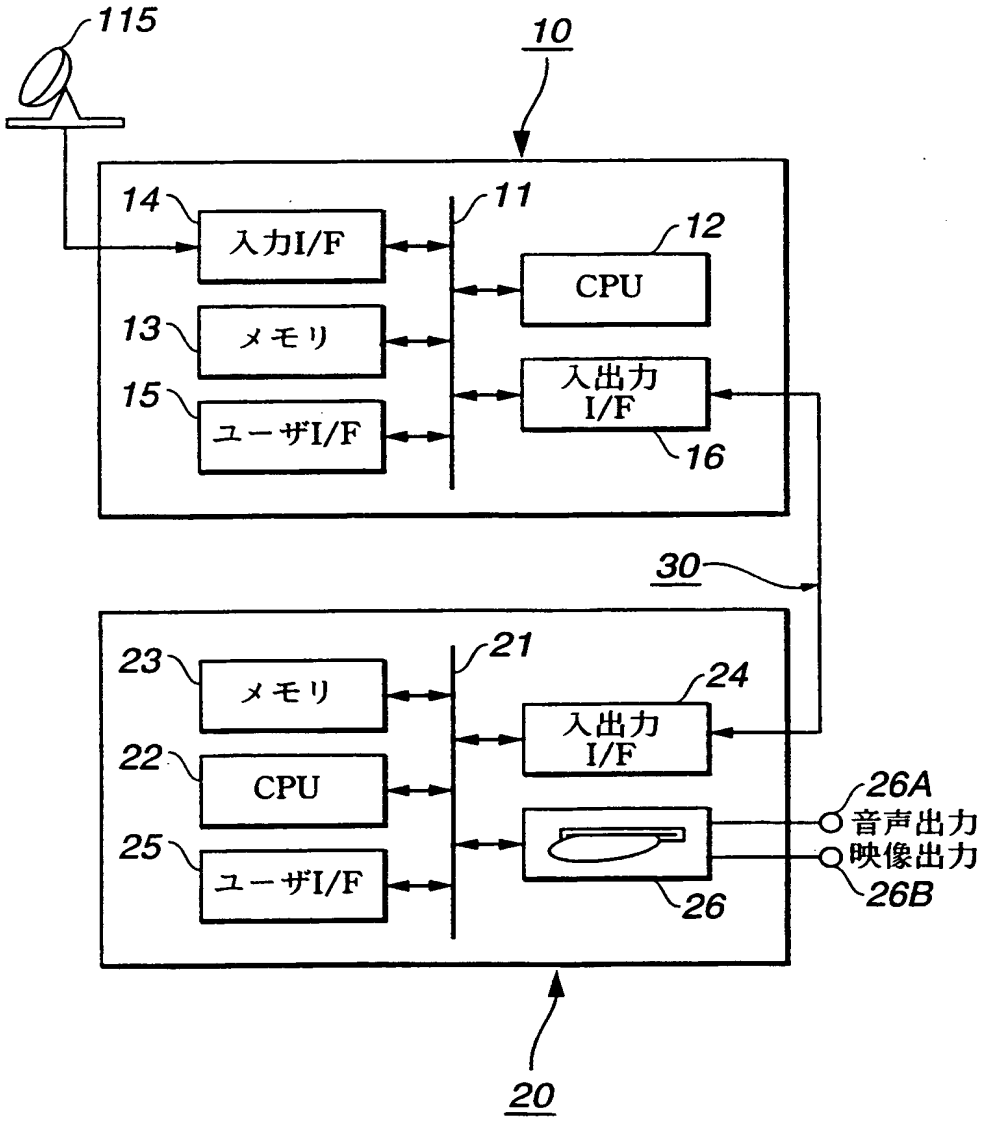

115
10
14
入力I/F
11
12
CPU
13
メモリ
15
ユーザI/F
入出力
I/F
16
30
23
メモリ
21
24
入出力
I/F
22
CPU
26A
音声出力
映像出力
25
ユーザI/F
26
26B
20

FIG.5

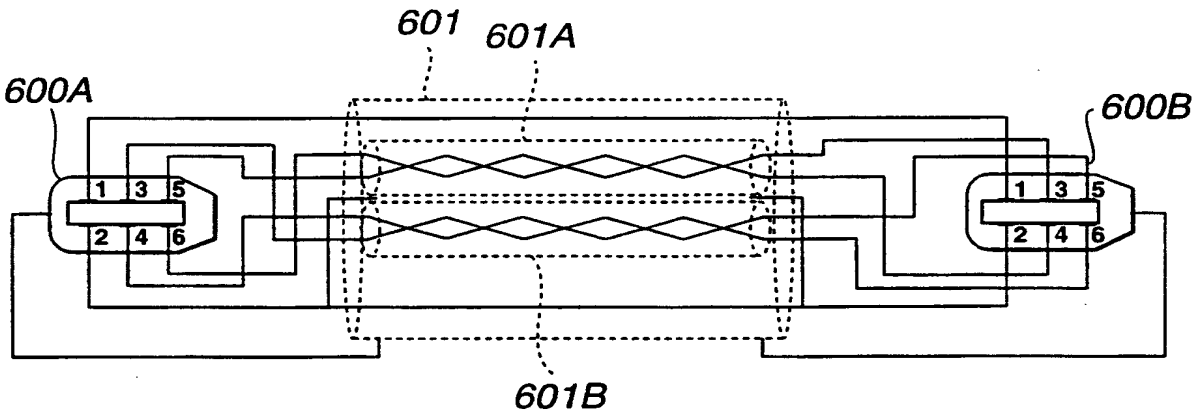


FIG.6

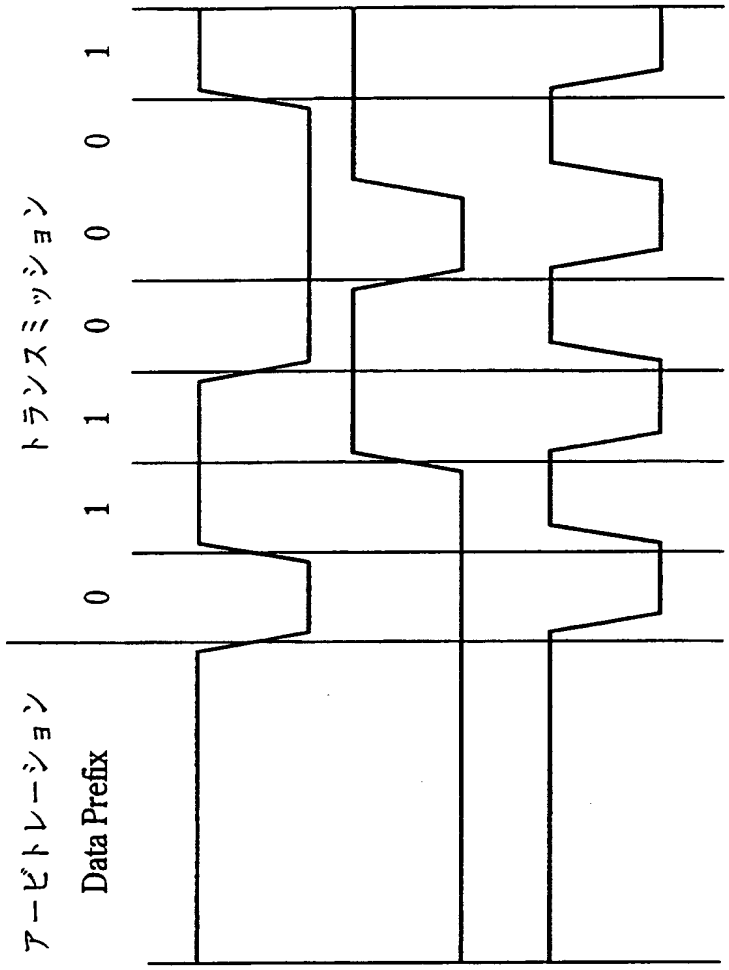


FIG.7A

FIG.7B

FIG.7C

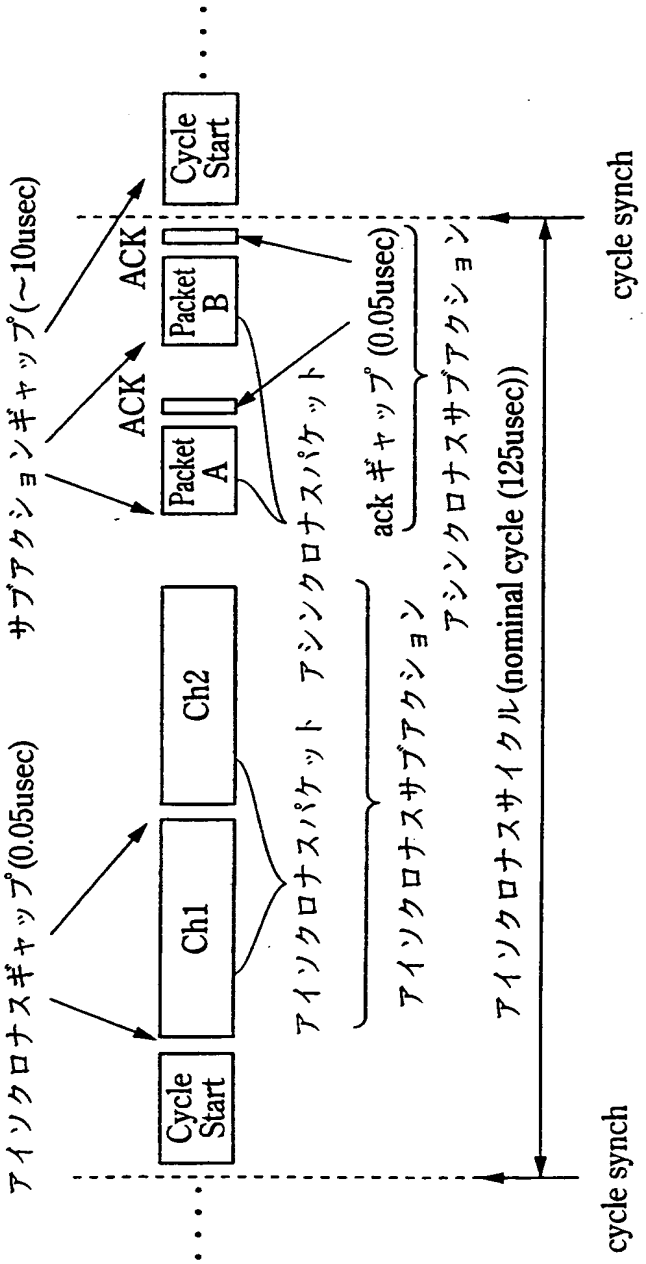

アイソクロナスギャップ(0.05usec)
サブアクションギャップ(~10usec)
Cycle Start
Ch1
Ch2
Packet A
ACK
Packet B
ACK
Cycle Start
アイソクロナスパケット
アシンクロナスパケット
ack ギャップ (0.05usec)
アイソクロナスサブアクション
アシンクロナスサブアクション
アイソクロナスサイクル(nominal cycle (125usec))
cycle synch
cycle synch

FIG.8

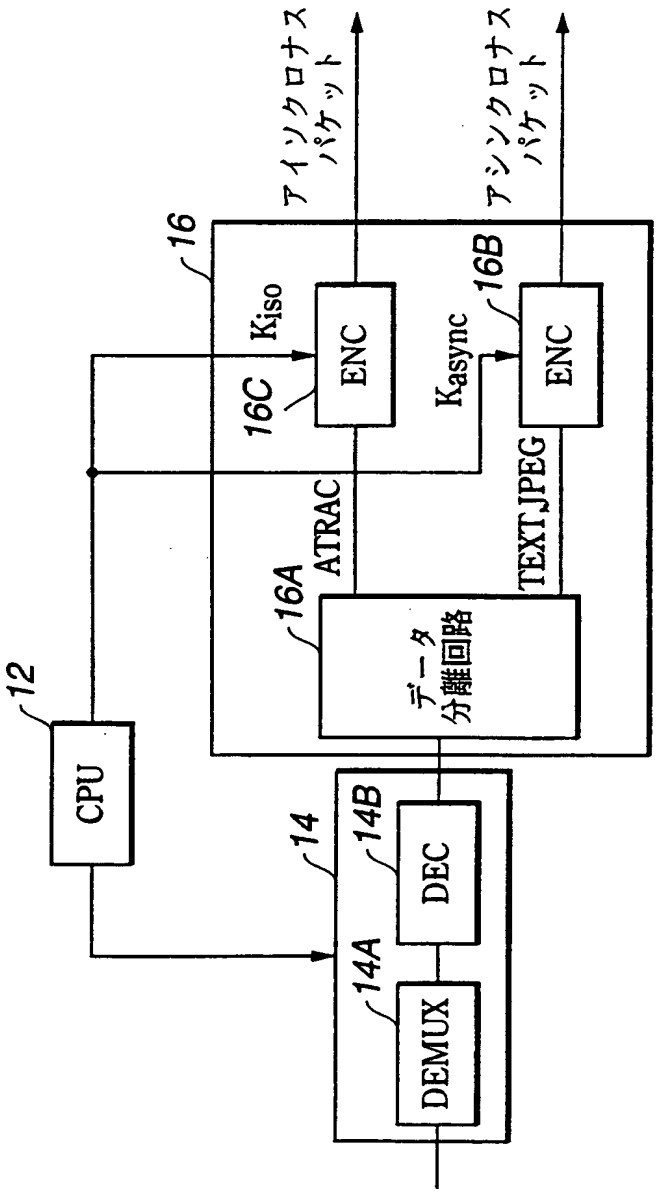

アイソクロナス パケット
アシンクロナス パケット
16
16B
Kiso
Kasync
16C
ENC
ENC
ATRAC
TEXT JPEG
16A
データ 分離回路
12
CPU
14
14B
DEC
14A
DEMUX

FIG.9

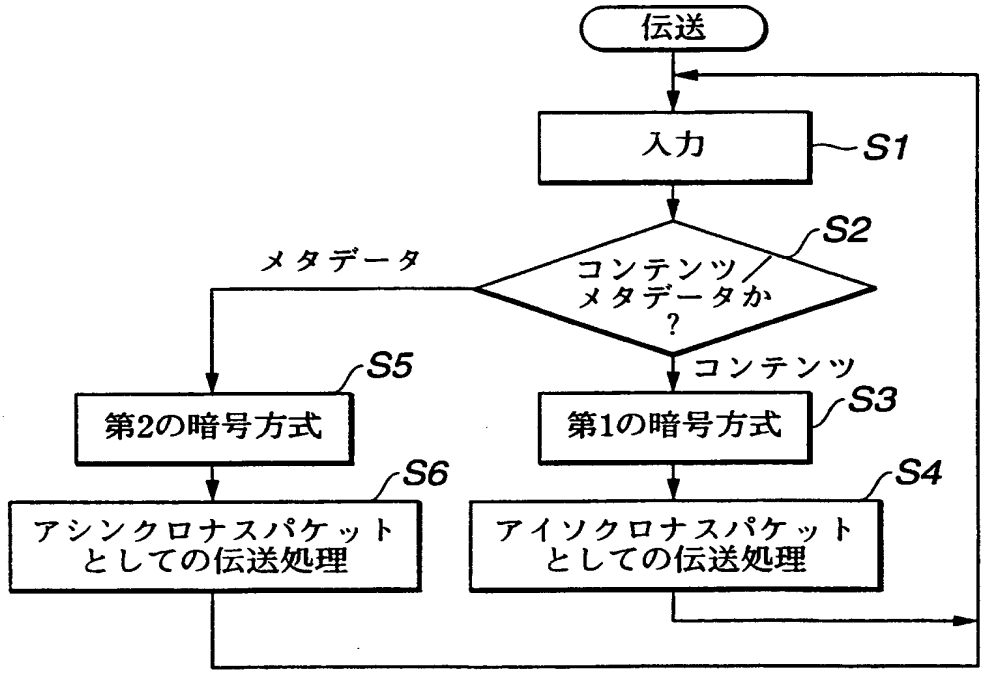

伝送
入力
S1
S2
コンテンツ／メタデータか？
メタデータ
コンテンツ
S5
第2の暗号方式
S3
第1の暗号方式
S6
アシンクロナスパケットとしての伝送処理
S4
アイソクロナスパケットとしての伝送処理

FIG.10

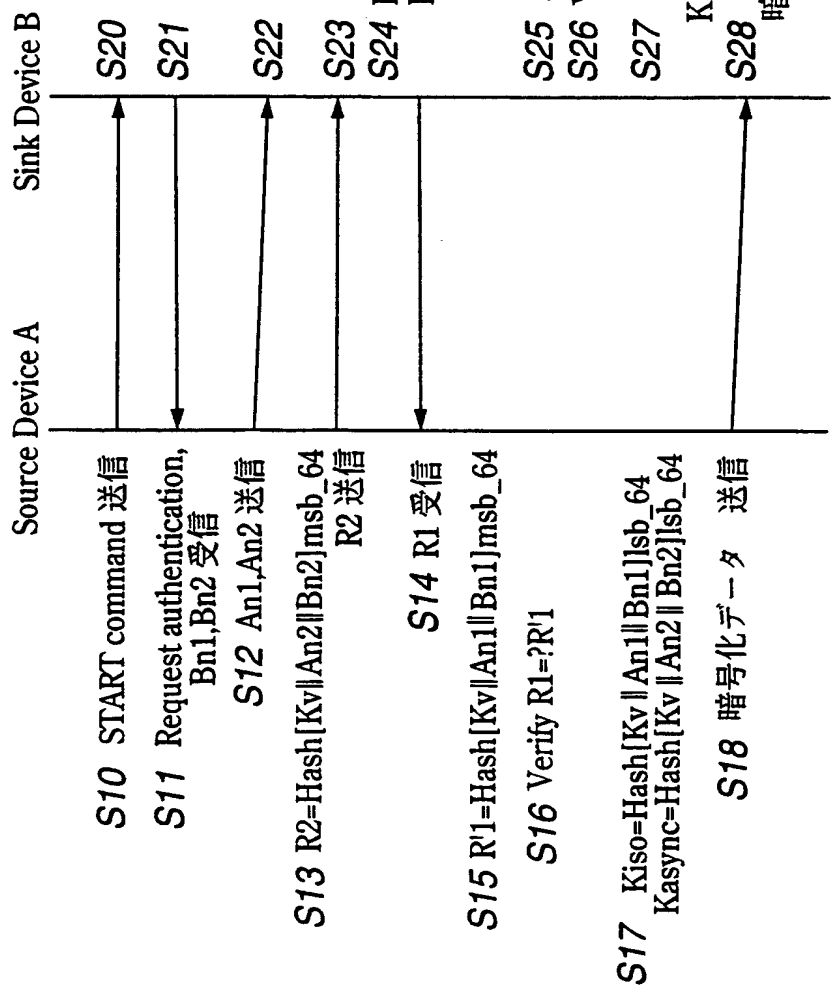

Source Device A
Sink Device B
S10 START command 送信
S20 START command 受信
S11 Request authentication, Bn1,Bn2 受信
S21 Request authentication, Bn1,Bn2 送信
S12 An1,An2 送信
S22 An1,An2 受信
S13 R2=Hash[Kv||An2||Bn2]msb_64 R2 送信
S23 R2 受信
S14 R1 受信
S24 R1=Hash[Kv||An1||Bn1]msb_64 R1 送信
S15 R'1=Hash[Kv||An1||Bn1]msb_64
S16 Verify R1=?R'1
S25 R'2=Hash[Kv||An2||Bn2]msb_64
S26 Verify R2=?R'2
S17 Kiso=Hash[Kv || An1||Bn1]lsb_64 Kasync=Hash[Kv || An2 || Bn2]lsb_64
S27 K'iso=Hash[Kv || An1|| Bn1]lsb_64 K'async=Hash[Kv || An2 || Bn2]lsb_64
S18 暗号化データ 送信
S28 暗号化データ 受信復号

FIG.11

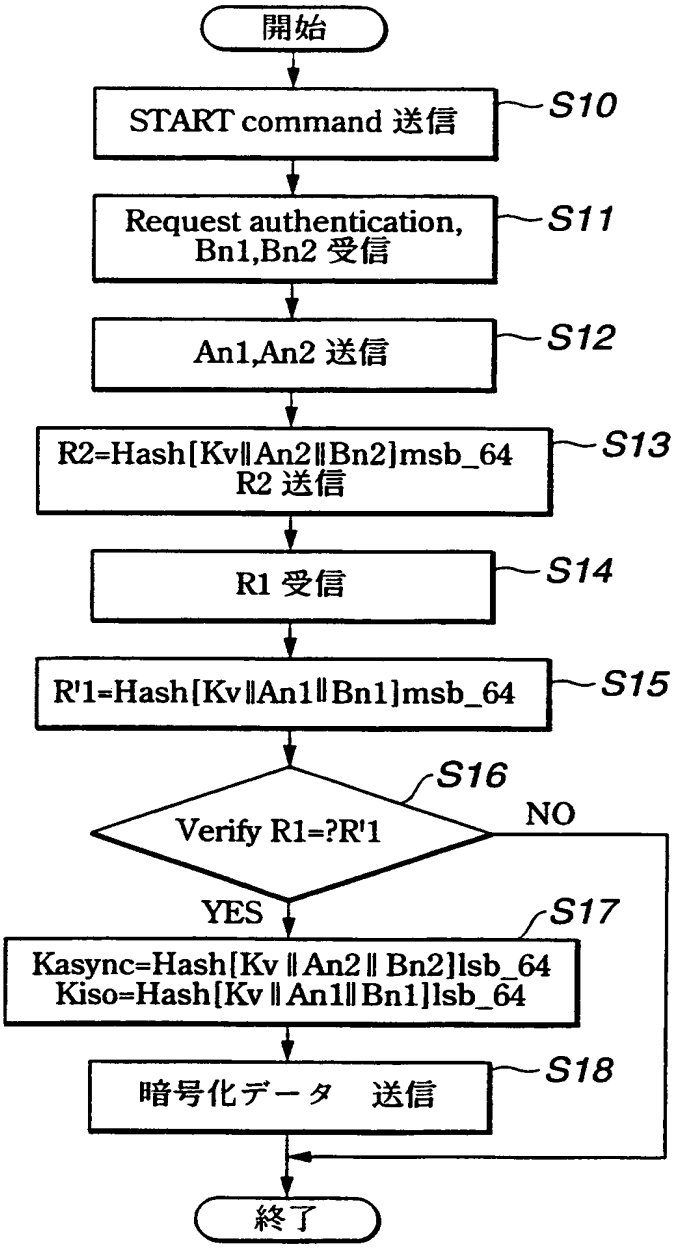

開始
START command 送信
S10
Request authentication,
Bn1,Bn2 受信
S11
An1,An2 送信
S12
R2=Hash[Kv‖An2‖Bn2]msb_64
R2 送信
S13
R1 受信
S14
R'1=Hash[Kv‖An1‖Bn1]msb_64
S15
S16
Verify R1=?R'1
NO
YES
S17
Kasync=Hash[Kv‖An2‖Bn2]lsb_64
Kiso=Hash[Kv‖An1‖Bn1]lsb_64
暗号化データ 送信
S18
終了

FIG.12

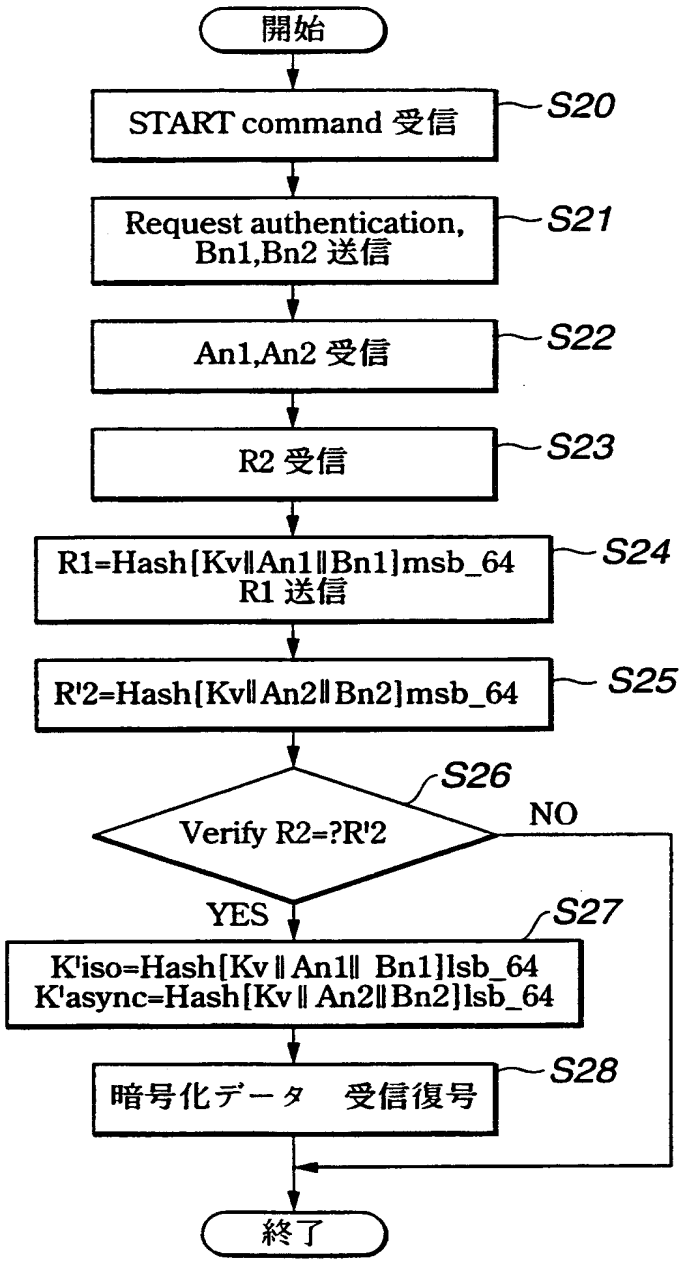

開始
START command 受信
S20
Request authentication, Bn1,Bn2 送信
S21
An1,An2 受信
S22
R2 受信
S23
R1=Hash[Kv‖An1‖Bn1]msb_64
R1 送信
S24
R'2=Hash[Kv‖An2‖Bn2]msb_64
S25
S26
Verify R2=?R'2
NO
YES
S27
K'iso=Hash[Kv‖An1‖ Bn1]lsb_64
K'async=Hash[Kv‖An2‖Bn2]lsb_64
暗号化データ 受信復号
S28
終了

FIG.13

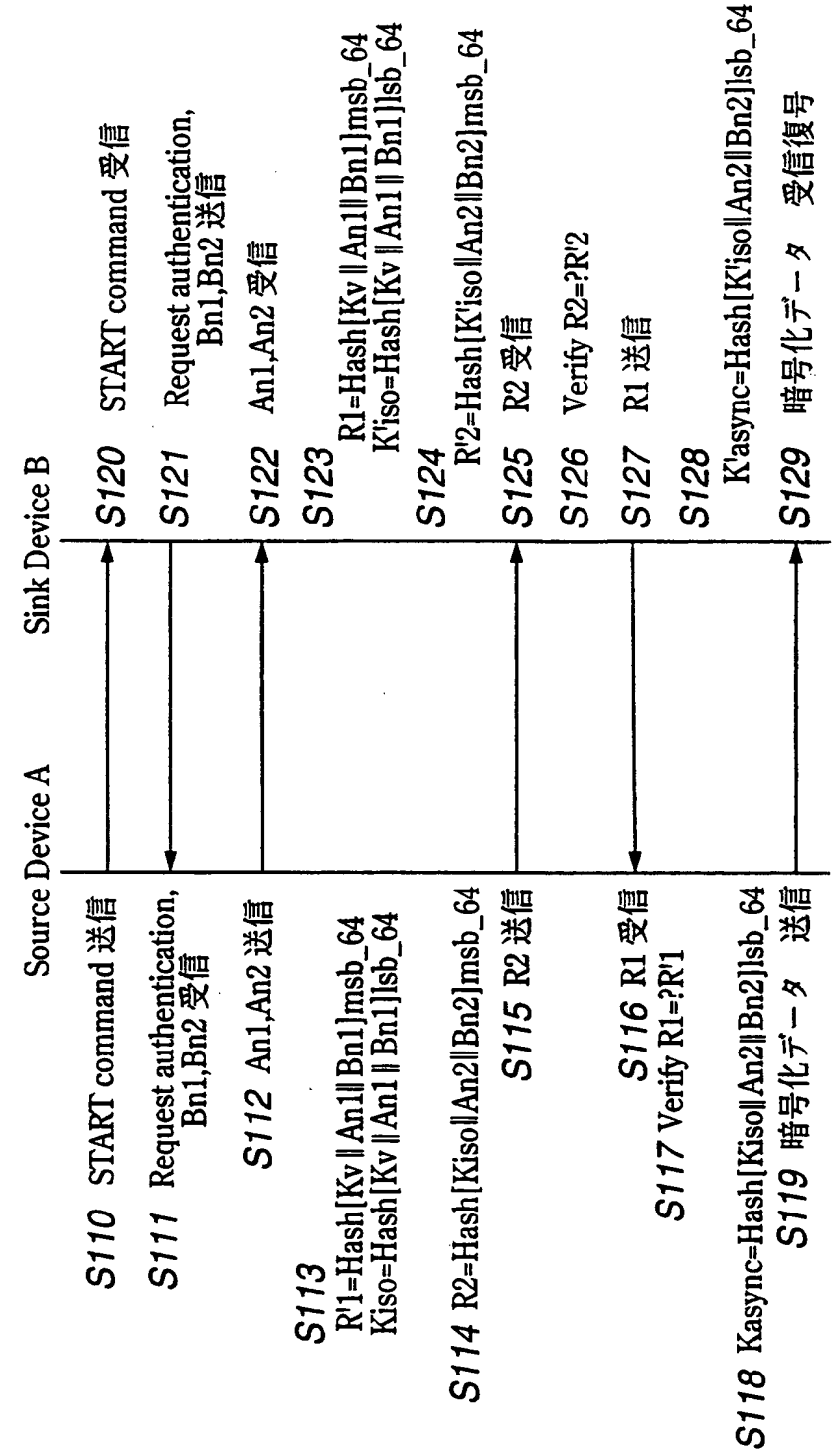

Source Device A
Sink Device B
S110 START command 送信
S120 START command 受信
S111 Request authentication, Bn1,Bn2 受信
S121 Request authentication, Bn1,Bn2 送信
S112 An1,An2 送信
S122 An1,An2 受信
S113
R'1=Hash[Kv‖An1‖Bn1]msb_64
Kiso=Hash[Kv‖An1‖Bn1]lsb_64
S123
R1=Hash[Kv‖An1‖Bn1]msb_64
K'iso=Hash[Kv‖An1‖Bn1]lsb_64
S114 R2=Hash[Kiso‖An2‖Bn2]msb_64
S124
R'2=Hash[K'iso‖An2‖Bn2]msb_64
S115 R2 送信
S125 R2 受信
S126 Verify R2=?R'2
S116 R1 受信
S127 R1 送信
S117 Verify R1=?R'1
S128
K'async=Hash[K'iso‖An2‖Bn2]lsb_64
S118 Kasync=Hash[Kiso‖An2‖Bn2]lsb_64
S119 暗号化データ 送信
S129 暗号化データ 受信復号

FIG.14

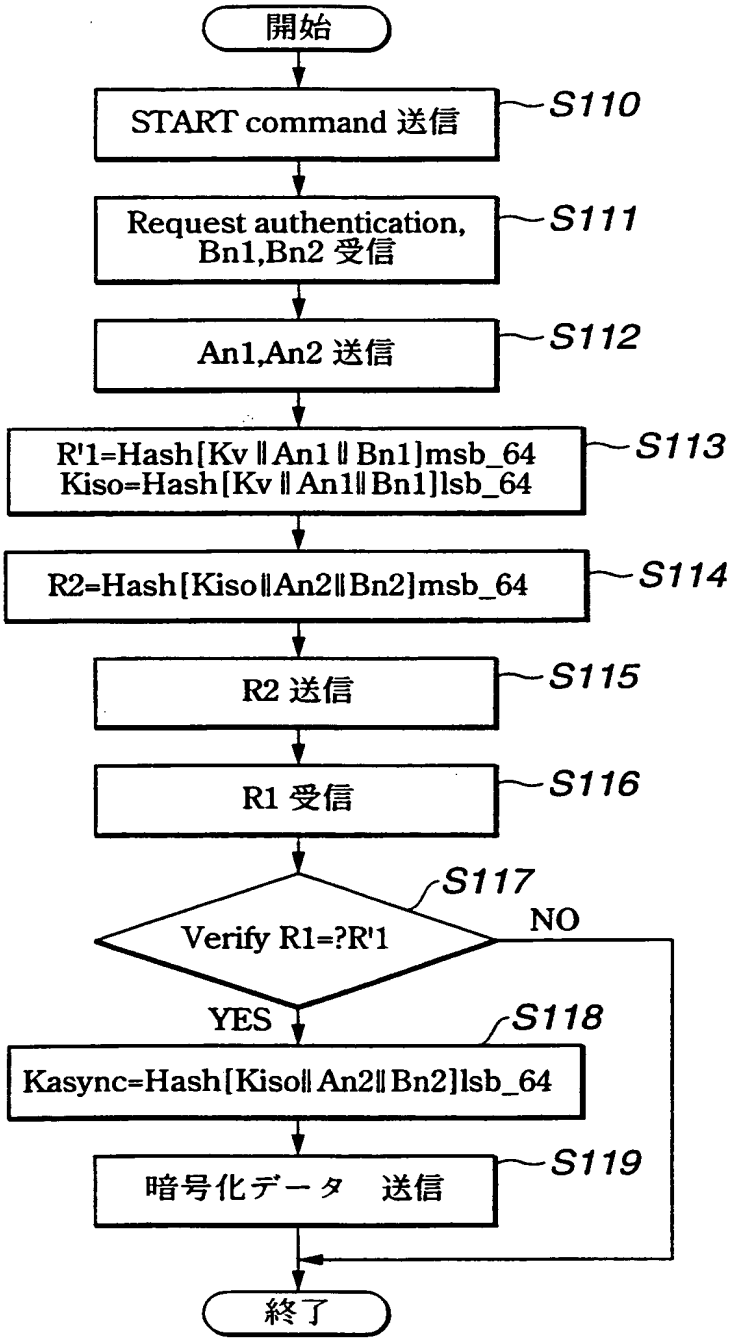

開始
START command 送信
S110
Request authentication, Bn1,Bn2 受信
S111
An1,An2 送信
S112
R'1=Hash[Kv‖An1‖Bn1]msb_64
Kiso=Hash[Kv‖An1‖Bn1]lsb_64
S113
R2=Hash[Kiso‖An2‖Bn2]msb_64
S114
R2 送信
S115
R1 受信
S116
Verify R1=?R'1
S117
NO
YES
Kasync=Hash[Kiso‖An2‖Bn2]lsb_64
S118
暗号化データ 送信
S119
終了

FIG.15

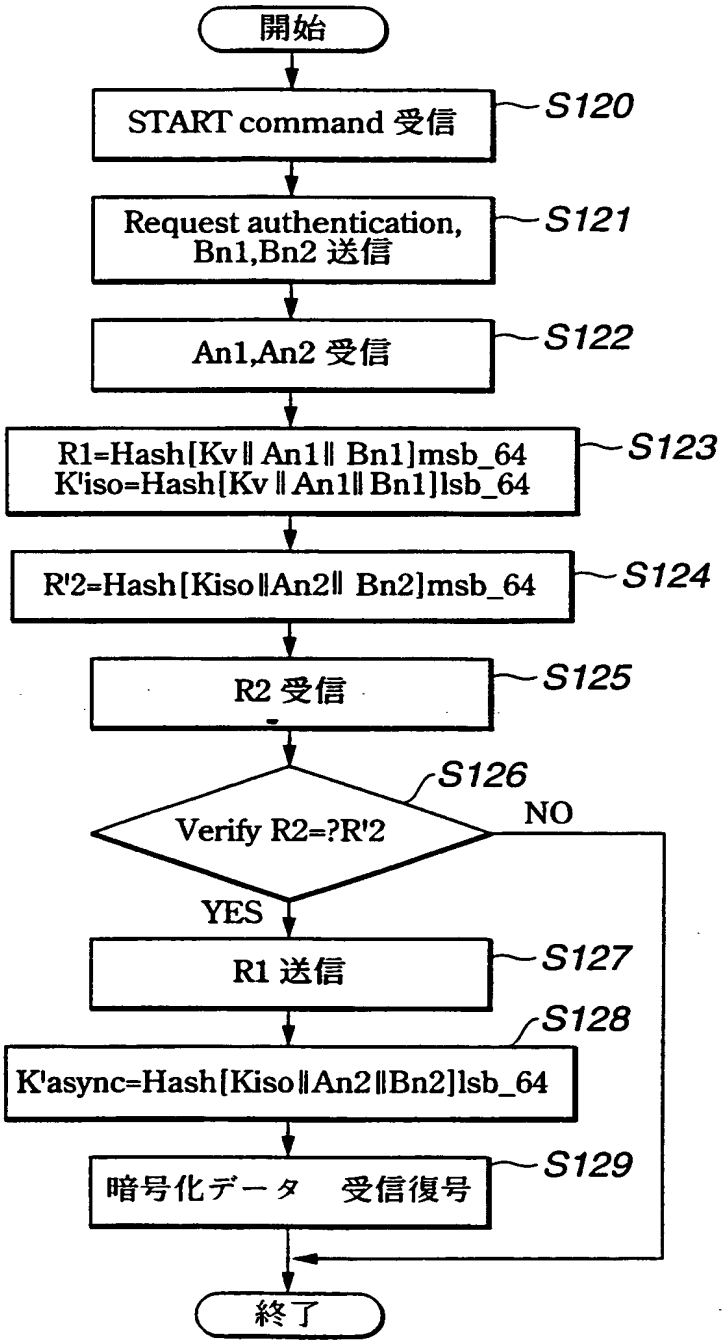

開始
START command 受信
S120
Request authentication, Bn1,Bn2 送信
S121
An1,An2 受信
S122
R1=Hash[Kv‖An1‖Bn1]msb_64
K'iso=Hash[Kv‖An1‖Bn1]lsb_64
S123
R'2=Hash[Kiso‖An2‖Bn2]msb_64
S124
R2 受信
S125
Verify R2=?R'2
S126
NO
YES
R1 送信
S127
K'async=Hash[Kiso‖An2‖Bn2]lsb_64
S128
暗号化データ 受信復号
S129
終了

FIG16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02353

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L 9/08 H04L 9/32 H04L 12/28 H04H1/00
H04N 7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G09C 1/00 - 5/00 H04K 1/00 - 3/00 H04L 9/00 H04L 12/00 G11B 20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST File(JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP, 11-53264, A (Sony Corporation), 26 February, 1999 (26.02.99), especially see Par. No.[0218], Fig. 37 & EP, 874300, A & KR, 98081632, A & CN, 1202659, A	1-17, 28-44, 55-71, 82-97 18-27, 45-54, 72-81, 98-107
Y A	JP, 10-224402, A (Toshiba Corporation), 21 August, 1998 (21.08.98), especially see Par. No. [0044], (Family: none)	1-17, 28-44, 55-71, 82-97 18-27,45-54, 72-81,98-107
Y	JP, 11-27315, A (Sanyo Electric Co., Ltd.), 29 January, 1999 (29.01.99), especially see Par. No. [0003], (Family: none)	3,30,57,84
Y	JP, 10-21645, A (Sony Corporation), 23 January, 1998 (23.01.98), especially see Par. Nos. [0011] to [0012], (Family: none)	3,30,57,84
Y	JP, 10-51439, A (Matsushita Electric Ind. Co., Ltd.), 20 February, 1998 (20.02.98),	6,33,60,87

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 June, 2000 (16.06.00)	04 July, 2000 (04.07.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02353

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	especially see Fig.3 & EP, 809379, A & TW, 333630, A & KR, 97076418, A	
Y A	JP, 10-210023, A (Oki Electric Industry Co., Ltd.), 07 August, 1998 (07.08.98), especially see Fig.2, Par. No.[0138], (Family: none)	7-16, 34-43, 61-70, 88-97 18-27, 45-54, 72-81, 98-107
Y A	Hideki Tsubakiyama and Keiichiro Koga, "Security for Information Data Broadcasting System with Conditional-Access Control," 1993 Conference Record. IEEE GLOBECOM, Vol.1, (1993), pp.164-170, especially see Fig.3, Fig.4	9,11,13,15, 17,36,38,40, 42,44,63,65, 67,69,71,90, 92,94,96 18-27,45-54, 72-81,98-107
A	JP, 10-303945, A (Sony Corporation), 13 November, 1998 (13.11.98) & EP, 874503, A & KR, 98081633, A	2-5,29-32, 56-59,83-86
A	JP, 10-224763, A (Matsushita Electric Ind. Co., Ltd.), 21 August, 1998 (21.08.98) & EP, 858183, A & KR, 98071098, A	1-5,28-32, 55-59,82-86
A	Masanori Suzuki et al. "Eizou Kaigi System you Kosoku Serial Bus (IEEE 1394) Tsushin Houshiki" Joho Shori Gakkai Hokoku, Vol.96, No.12, (1996), pp.215-220 (96-DPS-74)	3,4,30,31, 57,58,84,85
A	JP, 9-74408, A (Nippon Telegr. & Teleph. Corp. <NTT>), 18 March, 1997 (18.03.97) (Family: none)	6-27,33-54, 60-81,87-107
A	JP, 7-264668, A (Kokusai Denshin Denwa Co., Ltd. (KDD), 13 October, 1995 (13.10.95) & EP, 673178, A & US, 5596641, A	7-16,18-27, 34-43,45-54, 61-70,72-81, 88-107

国際調査報告

国際出願番号　PCT／JP00／02353

A.　発明の属する分野の分類（国際特許分類（IPC））
Int.Cl⁷　H04L 9／08　H04L 9／32　H04L 12／28　H04H1／00
H04N 7／167

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int.Cl⁷　G09C 1／00 － 5／00　H04K 1／00 － 3／00　H04L 9／00
H04L 12／00　G11B 20／10

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JICSTファイル（JOIS）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y A	JP，11－53264，A（ソニー株式会社） 26．2月．1999（26．02．99）， 特に第0218段落及び図37参照 & EP，874300，A & KR，98081632，A & CN，1202659，A	1-17, 28-44, 55-71, 82-97 18-27, 45-54, 72-81, 98-107
Y A	JP，10－224402，A（株式会社東芝） 21．8月．1998（21．08．98）， 特に第0044段落参照， （ファミリーなし）	1-17, 28-44, 55-71, 82-97 18-27, 45-54, 72-81, 98-107

☑ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
16．06．00	04.07.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	丸山　高政 印	5W　9570
	電話番号　03－3581－1101　内線　3576	

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２３５３

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，１１－２７３１５，Ａ（三洋電機株式会社） ２９．１月．１９９９（２９．０１．９９）， 特に第０００３段落参照，（ファミリーなし）	3, 30, 57, 84
Ｙ	ＪＰ，１０－２１６４５，Ａ（ソニー株式会社） ２３．１月．１９９８（２３．０１．９８）， 特に第００１１～００１２段落を参照，（ファミリーなし）	3, 30, 57, 84
Ｙ	ＪＰ，１０－５１４３９，Ａ（松下電器産業株式会社） ２０．２月．１９９８（２０．０２．９８），特に図３参照 ＆　ＥＰ，８０９３７９，Ａ　＆　ＴＷ，３３３６３０，Ａ ＆　ＫＲ，９７０７６４１８，Ａ	6, 33, 60, 87
Ｙ Ａ	ＪＰ，１０－２１００２３，Ａ（沖電気工業株式会社） ７．８月．１９９８（０７．０８．９８）， 特に図２及び第０１３８段落参照，（ファミリーなし）	7-16, 34-43, 61-70, 88-97 18-27, 45-54, 72-81, 98-107
Ｙ Ａ	Hideki Tsubakiyama and Keiichiro Koga, “Security for Information Data Broadcasting System with Conditional-Access Control,” 1993 Conference Record. IEEE GLOBECOM, Vol. 1, (1993), pp. 164－170, 特にFig. 3及びFig. 4参照	9, 11, 13, 15, 17, 36, 38, 40, 42, 44, 63, 65, 67, 69, 71, 90, 92, 94, 96 18-27, 45-54, 72-81, 98-107
Ａ	ＪＰ，１０－３０３９４５，Ａ（ソニー株式会社） １３．１１月．１９９８（１３．１１．９８） ＆　ＥＰ，８７４５０３，Ａ　＆　ＫＲ，９８０８１６３３，Ａ	2-5, 29-32, 56-59, 83-86
Ａ	ＪＰ，１０－２２４７６３，Ａ（松下電器産業株式会社） ２１．８月．１９９８（２１．０８．９８） ＆　ＥＰ，８５８１８３，Ａ　＆　ＫＲ，９８０７１０９８，Ａ	1-5, 28-32, 55-59, 82-86
Ａ	鈴木昌則，藤本卓也，影山敏宏，北山洋幸，小泉寿男“映像会議システム用高速シリアルバス(IEEE 1394)通信方式”情報処理学会研究報告，Vol. 96, No. 12, (1996), pp. 215－220 (96-DPS-74)	3, 4, 30, 31, 57, 58, 84, 85
Ａ	ＪＰ，９－７４４０８，Ａ（日本電信電話株式会社） １８．３月．１９９７（１８．０３．９７），（ファミリーなし）	6-27, 33-54, 60-81, 87-107
Ａ	ＪＰ，７－２６４６８，Ａ（国際電信電話株式会社） １３．１０月．１９９５（１３．１０．９５） ＆　ＥＰ，６７３１７８，Ａ　＆　ＵＳ，５５９６６４１，Ａ	7-16, 18-27, 34-43, 45-54, 61-70, 72-81, 88-107